Internet e architetture di rete

Antonio Prado
https://www.prado.it

Ciclo di seminari - Calendario

Internet: Sistemi autonomi e Governance

07 aprile 2016

Addio IPv4, Benvenuto IPv6

14 aprile 2016

Architetture di instradamento a Internet: il BGP

21 aprile 2016

Numeri e Nomi: il DNS

28 aprile 2016

34 anni di e-mail: SMTP

05 maggio 2016

Numeri e Nomi: il DNS

Domain name system

ICANN

gTLD

.com
.net
.org
.biz
.info
...

neustar

ccTLD

.it
.eu
.de
.ch
.tv
...

Registro.it

.eu
Your European Identity

TCP/UDP 53

[Paul_Mockapetris]

Paul Mockapetris, Internet pioneer

[RFC 822, 883, 973, **1034, 1035**, 1101, 1183]

Le definizioni

RFC Editor

RFC	Type	Status	Title
882		Obsolete	Domain Names – Concepts and Facilities
883		Obsolete	Domain Names – Implementation and Specification
920			Domain Requirements
973		Obsolete	Domain System Changes and Observations
1032			Domain Administrators Guide
1033			Domain Administrators Operations Guide
1034	Standard		Domain Names – Concepts and Facilities
1035	Standard		Domain Names – Implementation and Specification
1101			DNS Encoding of Network Names and Other Types
1123	Standard		Requirements for Internet Hosts – Application and Support
1178	Informational		Choosing a Name for Your Computer
1183	Experimental		New DNS RR Definitions
1348	Experimental	Obsolete	DNS NSAP RRs
1401	Informational		Correspondence between the IAB and DISA on the use of DNS throughout the Internet
1535	Informational		A Security Problem and Proposed Correction With Widely Deployed DNS Software
1536	Informational		Common DNS Implementation Errors and Suggested Fixes
1537	Informational	Obsolete	Common DNS Data File Configuration Errors
1591	Informational		Domain Name System Structure and Delegation
1611	Historic	Historic	DNS Server MIB Extensions
1612	Historic	Historic	DNS Resolver MIB Extensions

1983

1994

Le definizioni

RFC Editor

RFC	Type	Status	Title
1637	Experimental	Obsolete	DNS NSAP Resource Records
1664	Experimental	Obsolete	Using the Internet DNS to Distribute RFC1327 Mail Address Mapping Tables
1706	Informational		DNS NSAP Resource Records
1712	Experimental		DNS Encoding of Geographical Location
1713	Informational		Tools for DNS Debugging
1794	Informational		DNS Support for Load Balancing
1876	Experimental		A Means for Expressing Location Information in the Domain Name System
1886	Proposed	Obsolete	DNS Extensions to support IP version 6
1912	Informational		Common DNS Data File Configuration Errors
1982	Proposed		Serial Number Arithmetic
1995	Proposed		Incremental Zone Transfer in DNS
1996	Proposed		A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
2010	Informational	Obsolete	Operational Criteria for Root Name Servers
2052	Experimental	Obsolete	A DNS RR for specifying the location of services (DNS SRV)
2065	Proposed	Obsolete	Domain Name System Security Extensions
2100	Informational	April 1st	The Naming of Hosts
2136	Proposed		Dynamic Updates in the Domain Name System (DNS UPDATE)
2137	Proposed	Obsolete	Secure Domain Name System Dynamic Update
2163	Proposed		Using the Internet DNS to Distribute MIXER Conformant Global Address Mapping (MCGAM)
2168	Experimental	Obsolete	Resolution of Uniform Resource Identifiers using the Domain Name System

1994

1997

Le definizioni

RFC Editor

1997

RFC	Type	Status	Title
2181	Proposed		Clarifications to the DNS Specification
2182	BCP		Selection and Operation of Secondary DNS Servers
2230	Informational		Key Exchange Delegation Record for the DNS
2308	Proposed		Negative Caching of DNS Queries (DNS NCACHE)
2317	BCP		Classless IN-ADDR.ARPA delegation
2535	Proposed	Obsolete	Domain Name System Security Extensions
2536	Proposed		DSA KEYs and SIGs in the Domain Name System (DNS)
2537	Proposed	Obsolete	RSA/MD5 KEYs and SIGs in the Domain Name System (DNS)
2538	Proposed	Obsolete	Storing Certificates in the Domain Name System (DNS)
2539	Proposed		Storage of Diffie-Hellman Keys in the Domain Name System (DNS)
2540	Experimental		Detached Domain Name System (DNS) Information
2541	Informational	Obsolete	DNS Security Operational Considerations
2606	BCP		Reserved Top Level DNS Names
2671	Proposed	Obsolete	Extension Mechanisms for DNS (EDNS0)
2672	Proposed	Obsolete	Non-Terminal DNS Name Redirection
2673	Historic	Obsolete	Binary Labels in the Domain Name System
2782	Proposed		A DNS RR for specifying the location of services (DNS SRV)
2825	Informational		A Tangled Web: Issues of I18N, Domain Names, and the Other Internet protocols
2826	Informational		IAB Technical Comment on the Unique DNS Root
2845	Proposed		Secret Key Transaction Authentication for DNS (TSIG)

2000

Le definizioni

RFC Editor

2000

RFC	Type	Status	Title
2870	BCP		Root Name Server Operational Requirements
2874	Historic	Historic	DNS Extensions to Support IPv6 Address Aggregation and Renumbering
2915	Proposed	Obsolete	The Naming Authority Pointer (NAPTR) DNS Resource Record
2929	BCP	Obsolete	Domain Name System (DNS) IANA Considerations
2930	Proposed		Secret Key Establishment for DNS (TKEY RR)
2931	Proposed		DNS Request and Transaction Signatures (SIG(0)s)
3007	Proposed		Secure Domain Name System (DNS) Dynamic Update
3008	Proposed	Obsolete	Domain Name System Security (DNSSEC) Signing Authority
3071	Informational		Reflections on the DNS, RFC 1591, and Categories of Domains
3090	Proposed	Obsolete	DNS Security Extension Clarification on Zone Status
3110	Proposed		RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)
3123	Experimental		A DNS RR Type for Lists of Address Prefixes (APL RR)
3130	Informational		Notes from the State-Of-The-Technology: DNSSEC
3152	BCP	Obsolete	Delegation of IP6.ARPA
3197	Informational		Applicability Statement for DNS MIB Extensions
3225	Proposed		Indicating Resolver Support of DNSSEC
3226	Proposed		DNSSEC and IPv6 A6 aware server/resolver message size requirements
3258	Informational		Distributing Authoritative Name Servers via Shared Unicast Addresses
3363	Informational		Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS)
3364	Informational		Tradeoffs in Domain Name System (DNS) Support for Internet Protocol version 6 (IPv6)

2002

Le definizioni

RFC	Type	Status	Title
3403	Proposed		Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database
3425	Proposed		Obsoleting IQUERY
3445	Proposed	Obsolete	Limiting the Scope of the KEY Resource Record (RR)
3467	Informational		Role of the Domain Name System (DNS)
3490	Proposed	Obsolete	Internationalizing Domain Names in Applications (IDNA)
3491	Proposed	Obsolete	Nameprep: A Stringprep Profile for Internationalized Domain Names (IDN)
3492	Proposed		Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)
3596	Draft		DNS Extensions to Support IP Version 6
3597	Proposed		Handling of Unknown DNS Resource Record (RR) Types
3645	Proposed		Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)
3655	Proposed	Obsolete	Redefinition of DNS Authenticated Data (AD) bit
3658	Proposed	Obsolete	Delegation Signer (DS) Resource Record (RR)
3696	Informational		Application Techniques for Checking and Transformation of Names
3755	Proposed	Obsolete	Legacy Resolver Compatibility for Delegation Signer (DS)
3757	Proposed	Obsolete	Domain Name System KEY (DNSKEY) Resource Record (RR) Secure Entry Point (SEP) Flag
3833	Informational		Threat Analysis of the Domain Name System (DNS)
3845	Proposed	Obsolete	DNS Security (DNSSEC) NextSECure (NSEC) RDATA Format
3901	BCP		DNS IPv6 Transport Operational Guidelines
4025	Proposed		A Method for Storing IPsec Keying Material in DNS
4033	Proposed		DNS Security Introduction and Requirements

RFC Editor

2002

2005

Le definizioni

RFC Editor

RFC	Type	Status	Title
4034	Proposed		Resource Records for the DNS Security Extensions
4035	Proposed		Protocol Modifications for the DNS Security Extensions
4074	Informational		Common Misbehavior Against DNS Queries for IPv6 Addresses
4159	BCP		"Deprecation of "ip6.int"
4185	Informational		National and Local Characters for DNS Top Level Domain (TLD) Names
4255	Proposed		Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints
4339	Informational		IPv6 Host Configuration of DNS Server Information Approaches
4343	Proposed		Domain Name System (DNS) Case Insensitivity Clarification
4367	Informational		What's in a Name: False Assumptions about DNS Names
4398	Proposed		Storing Certificates in the Domain Name System (DNS)
4408	Experimental		Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1
4431	Informational		The DNSSEC Lookaside Validation (DLV) DNS Resource Record
4470	Proposed		Minimally Covering NSEC Records and DNSSEC On-line Signing
4471	Experimental		Derivation of DNS Name Predecessor and Successor
4472	Informational		Operational Considerations and Issues with IPv6 DNS
4509	Proposed		Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (Rrs)
4592	Proposed		The Role of Wildcards in the Domain Name System
4635	Proposed		HMAC SHA TSIG Algorithm Identifiers
4641	Informational	Obsolete	DNSSEC Operational Practices
4697	BCP		Observed DNS Resolution Misbehavior

2005

2006

Le definizioni

RFC	Type	Status	Title
4701	Proposed		A DNS Resource Record (RR) for Encoding Dynamic Host Configuration Protocol (DHCP) Information (DHCID RR)
4892	Informational		Requirements for a Mechanism Identifying a Name Server Instance
4955	Proposed		DNS Security (DNSSEC) Experiments
4956	Experimental		DNS Security (DNSSEC) Opt-In
4986	Informational		Requirements Related to DNS Security (DNSSEC) Trust Anchor Rollover
5001	Proposed		DNS Name Server Identifier (NSID) Option
5011	Standard		Automated Updates of DNS Security (DNSSEC) Trust Anchors
5074	Informational		DNSSEC Lookaside Validation (DLV)
5155	Proposed		DNS Security (DNSSEC) Hashed Authenticated Denial of Existence
5205	Experimental		Host Identity Protocol (HIP) Domain Name System (DNS) Extension
5358	BCP		Preventing Use of Recursive Nameservers in Reflector Attacks
5395	BCP	Obsolete	Domain Name System (DNS) IANA Considerations
5452	Proposed		Measures for Making DNS More Resilient against Forged Answers
5507	Informational		Design Choices When Expanding the DNS
5625	BCP		DNS Proxy Implementation Guidelines
5702	Proposed		Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC
5855	BCP		Nameservers for IPv4 and IPv6 Reverse Zones
5864	Proposed		DNS SRV Resource Records for AFS
5890	Proposed		Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework
5891	Proposed		Internationalized Domain Names for Applications (IDNA): Protocol

RFC Editor

2006

2010

Le definizioni

RFC	Type	Status	Title
5933	Proposed		Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC
5936	Proposed		DNS Zone Transfer Protocol (AXFR)
5966	Proposed		DNS Transport over TCP – Implementation Requirements
6014	Proposed		Cryptographic Algorithm Identifier Allocation for DNSSEC
6147	Proposed		DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers
6168	Informational		Requirements for Management of Name Servers for the DNS
6195	BCP	Obsolete	Domain Name System (DNS) IANA Considerations
6303	BCP		Locally Served DNS Zones
6304	Informational		AS112 Nameserver Operations
6305	Informational		I'm Being Attacked by PRISONER.IANA.ORG!
6335	BCP		Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry
6563	Informational		Moving A6 to Historic Status
6604	Proposed		xNAME RCODE and Status Bits Clarification
6605	Proposed		Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC
6672	Proposed		DNAME Redirection in the DNS
6698	Proposed		The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA
6725	Proposed		DNS Security (DNSSEC) DNSKEY Algorithm IANA Registry Updates
6742	Experimental		DNS Resource Records for the Identifier-Locator Network Protocol (ILNP)
6761	Proposed		Special-Use Domain Names
6781	Informational		DNSSEC Operational Practices, Version 2

RFC Editor

2010

2012

Le definizioni

RFC	Type	Status	Title
6804	Historic	Historic	DISCOVER: Supporting Multicast DNS Queries
6840	Proposed		Clarifications and Implementation Notes for DNS Security (DNSSEC)
6841	Informational		A Framework for DNSSEC Policies and DNSSEC Practice Statements
6844	Proposed		DNS Certification Authority Authorization (CAA) Resource Record
6891	Standard		Extension Mechanisms for DNS (EDNS(0))
6895	BCP		Domain Name System (DNS) IANA Considerations
6912	Informational		Principles for Unicode Code Point Inclusion in Labels in the DNS
6944	Proposed		Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status
6975	Proposed		Signaling Cryptographic Algorithm Understanding in DNS Security Extensions (DNSSEC)
7043	Informational		Resource Records for EUI-48 and EUI-64 Addresses in the DNS
7085	Informational		Top-Level Domains That Are Already Dotless
7218	Standard		Adding Acronyms to Simplify Conversations about DNS-Based Authentication of Named Entities (DANE)
7314	Informational		Extension Mechanisms for DNS (EDNS) EXPIRE Option
7344	Informational		Automating DNSSEC Delegation Trust Maintenance
7477	Standard		Child-to-Parent Synchronization in DNS
7534	Informational		AS112 Nameserver Operations
7535	Informational		AS112 Redirection Using DNAME
7583	Informational		DNSSEC Key Rollover Timing Considerations
7626	Informational		DNS Privacy Considerations
7646	Informational		Definition and Use of DNSSEC Negative Trust Anchors

RFC Editor

2012

2015

Le definizioni

RFC Editor

RFC	Type	Status	Title
7671	Standard		The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance
7686	Standard		The ".onion" Special-Use Domain Name

Last modified: November 24, 2015 at 4:17 pm

TO BE CONTINUED

2015

?

IETF Working Groups related to DNS

Internet Area (int) **int Area Directors (ADs): Suresh Krishnan and Terry Manderson**

Group	Responsible AD	Name	Chairs
Dnssd	Terry	Extensions for Scalable DNS Service Discovery	Tim Chown, Ralph Droms
Dprive	Terry	DNS PRIVate Exchange	Warren Kumari, Tim Wicinski

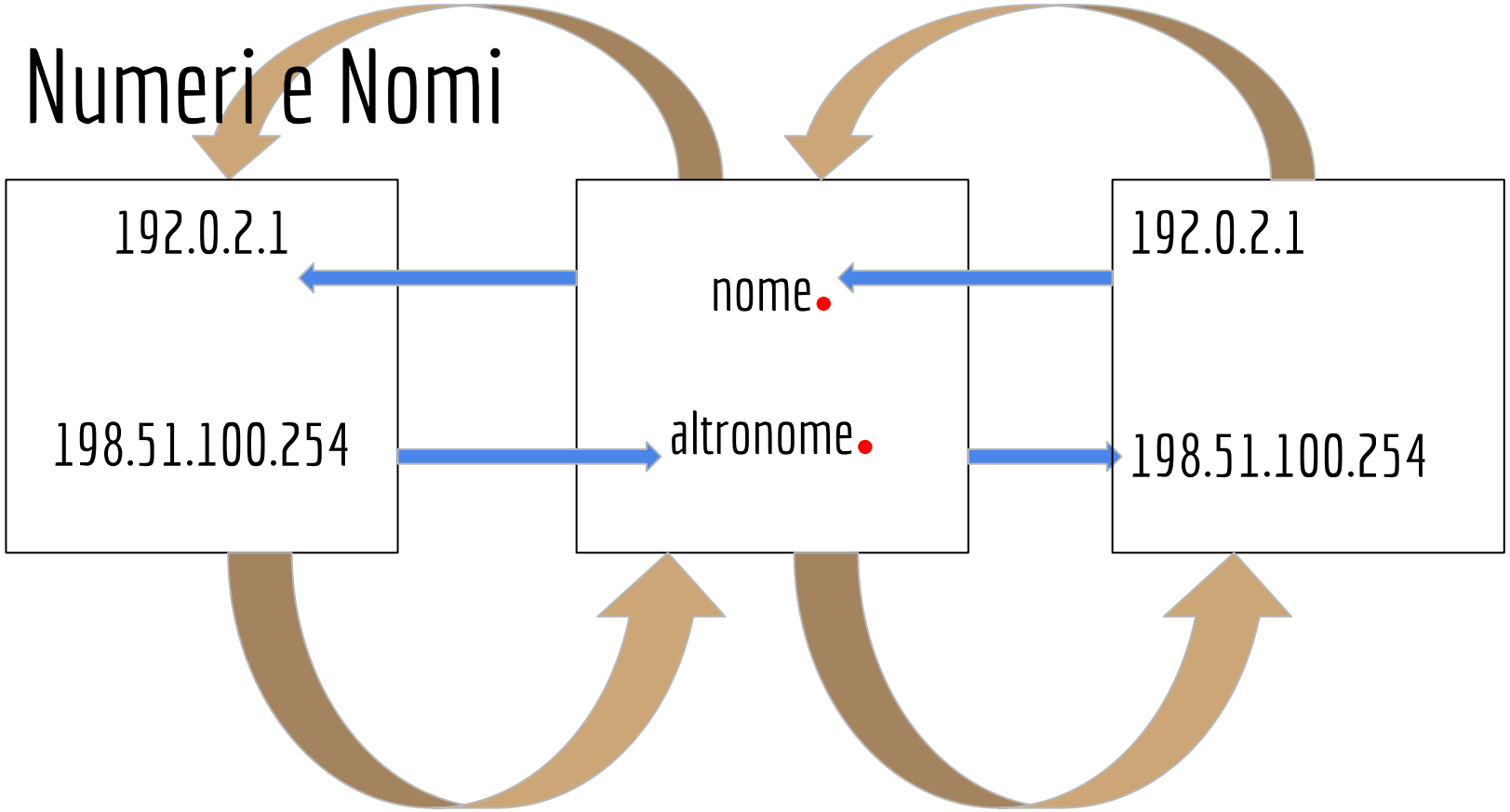
Operations and Management Area (ops) **ops Area Directors (ADs): Benoit Claise and Joel Jaeggli**

Group	Responsible AD	Name	Chairs
Dnsop	Joel	Domain Name System Operations	Tim Wicinski, Suzanne Woolf

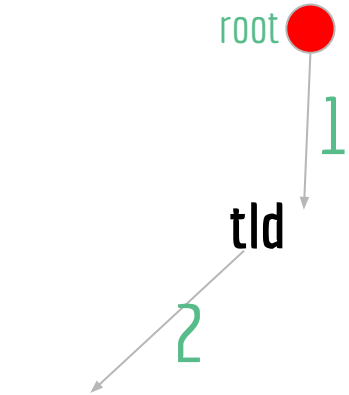
Security Area (sec) **sec Area Directors (ADs)** **Stephen Farrell and Kathleen Moriarty**

Group	Responsible AD	Name	Chairs
Dane	Stephen	DNS-based Authentication of Named Entities	Ólafur Guðmundsson, Warren Kumari

Numeri e Nomi



Il PUNTO



www . domain . tld . root

3 2 1

1 tld.
2 domain.tld.
3 my.domain.tld.
4 like.my.domain.tld.
5 you.like.my.domain.tld.
6 so.you.like.my.domain.tld.
7 hey.so.you.like.my.domain.tld.

I tre componenti del DNS

Domain name space e Resource Records

Gli elementi di una nomenclatura ad albero con dati associati ai nomi

Name Servers

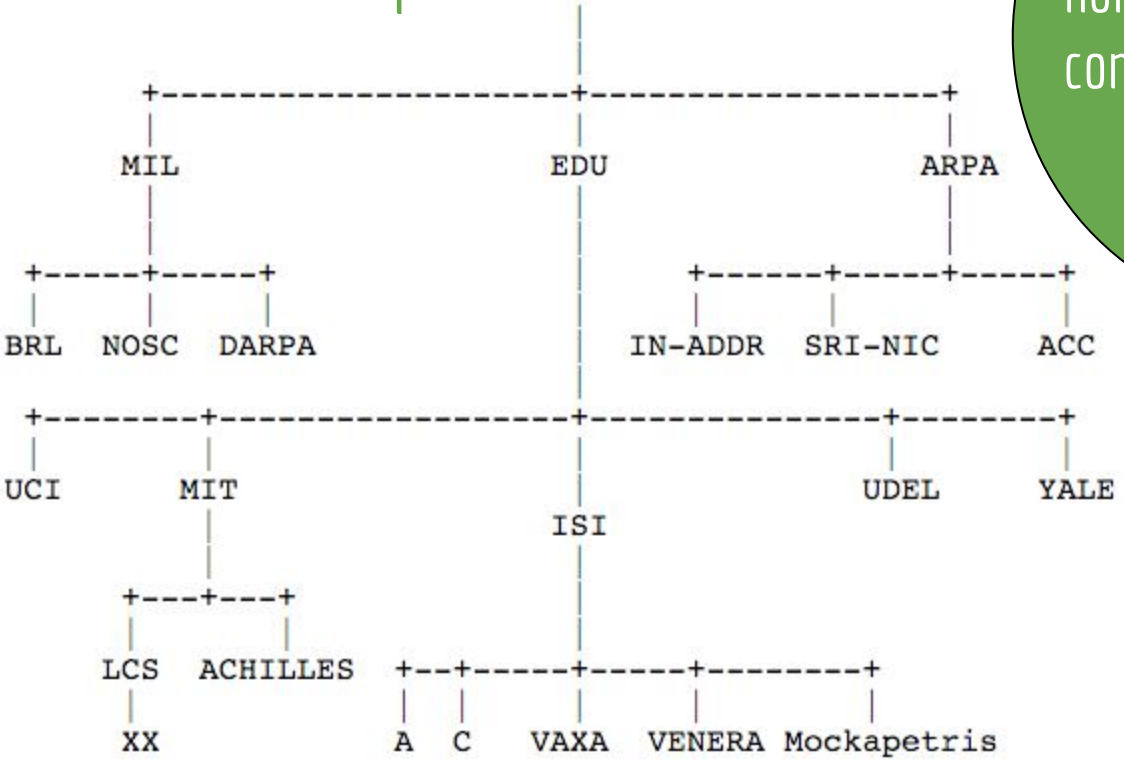
I programmi server che detengono le informazioni sulla struttura ad albero e il relativo insieme di dati

Resolvers

I programmi che estraggono le informazioni dai name server in risposta alle richieste dei client

I tre componenti del DNS

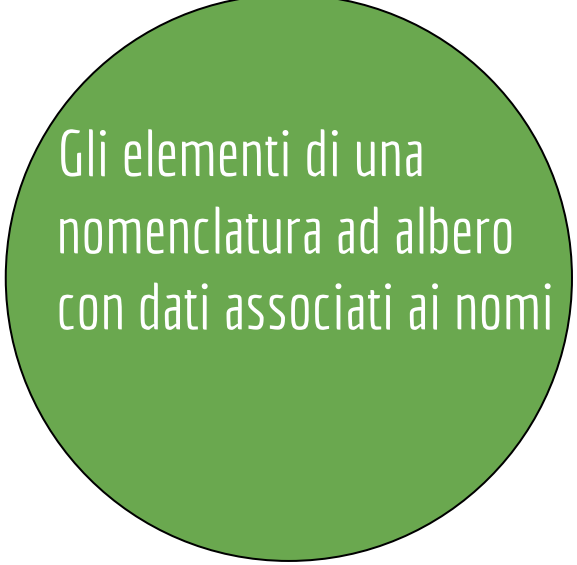
Domain name space e Resource Records



Gli elementi di una nomenclatura ad albero con dati associati ai nomi

I tre componenti del DNS

Domain name space e Resource Records



CLASS
- CH - chaos
- IN - internet

TYPE
- A - indirizzo di un host
- CNAME - alias di un host
- HINFO - informazioni su un host
- MX - server di posta per il dominio
- NS - name server autoritativo per il dominio
- PTR - puntatore a un'altra sezione del dominio
- SOA - origine dell'autorità per una zona
- TXT - stringa di testo

TTL
- Time To Live, durata di un Resource Record

I tre componenti del DNS

Domain name space e Resource Records

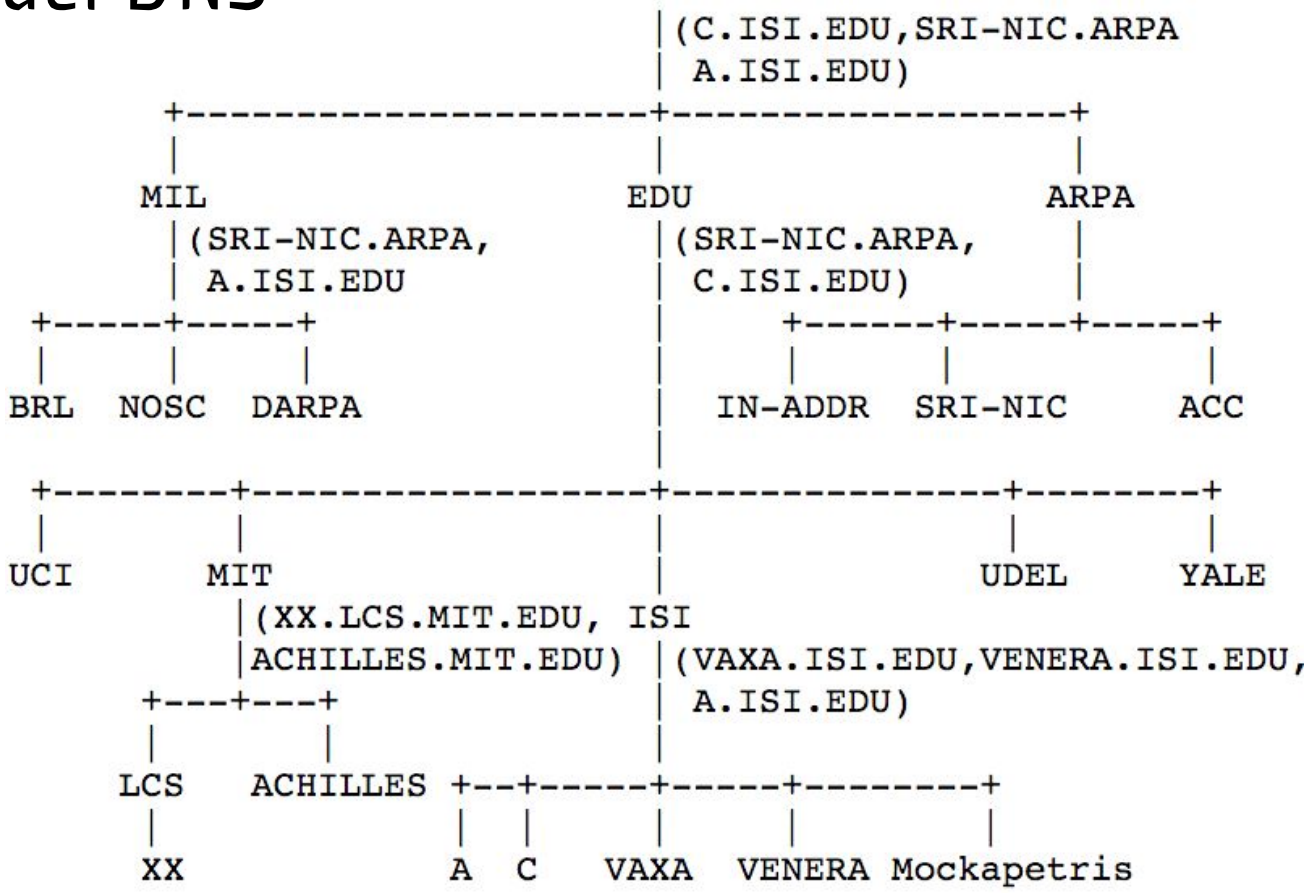
Gli elementi di una nomenclatura ad albero con dati associati ai nomi

```
XX.LCS.MIT.EDU.  IN      A       10.0.0.44
                 CH      A       MIT.EDU. 2420

ISI.EDU.         MX      10 VENERA.ISI.EDU.
                 MX      10 VAXA.ISI.EDU.
VENERA.ISI.EDU.  A       128.9.0.32
                 A       10.1.0.52
VAXA.ISI.EDU.    A       10.2.0.27
                 A       128.9.0.33
```

I tre componenti del DNS

Name Servers

I programmi server che detengono le informazioni sulla struttura ad albero e il relativo insieme di dati



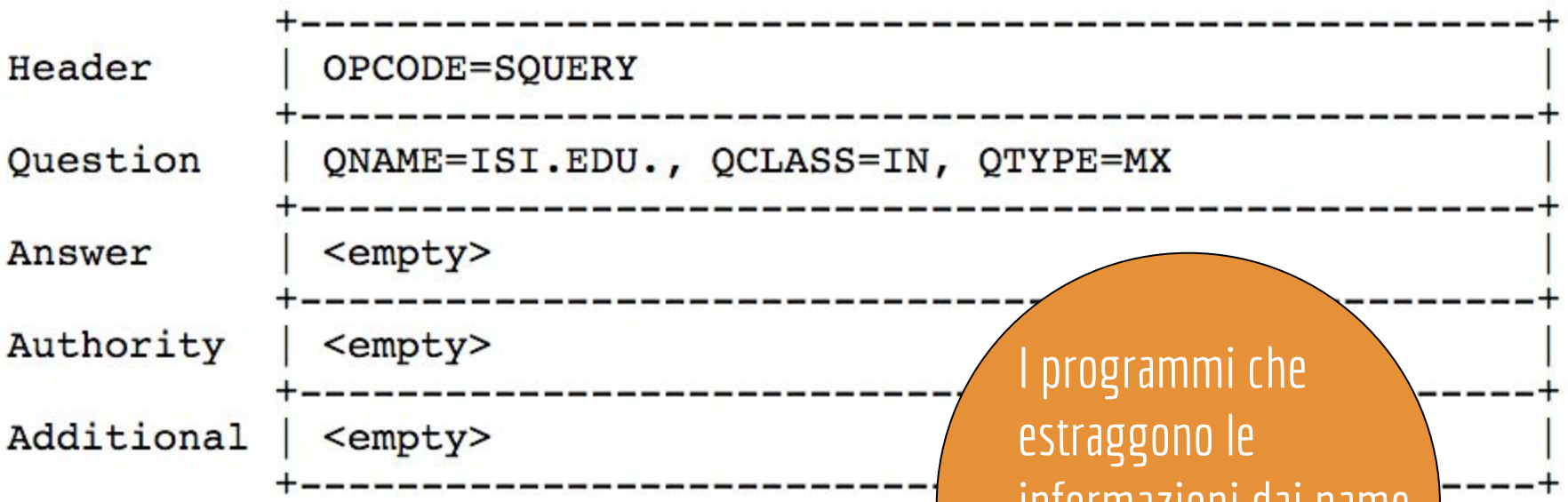
I tre componenti del DNS

Name Servers

I programmi server che detengono le informazioni sulla struttura ad albero e il relativo insieme di dati

```
.               IN      SOA     SRI-NIC.ARPA. HOSTMASTER.SRI-NIC.ARPA. (
                                870611          ;serial
                                1800            ;refresh every 30 min
                                300             ;retry every 5 min
                                604800          ;expire after a week
                                86400)          ;minimum of a day
                        NS      A.ISI.EDU.
                        NS      C.ISI.EDU.
                        NS      SRI-NIC.ARPA.

MIL.            86400   NS      SRI-NIC.ARPA.
                86400   NS      A.ISI.EDU.

EDU.            86400   NS      SRI-NIC.ARPA.
                86400   NS      C.ISI.EDU.

SRI-NIC.ARPA.           A       26.0.0.73
                        A       10.0.0.51
                        MX      0 SRI-NIC.ARPA.
                        HINFO   DEC-2060 TOPS20

ACC.ARPA.               A       26.6.0.65
                        HINFO   PDP-11/70 UNIX
                        MX      10 ACC.ARPA.

USC-ISIC.ARPA.          CNAME   C.ISI.EDU.
```

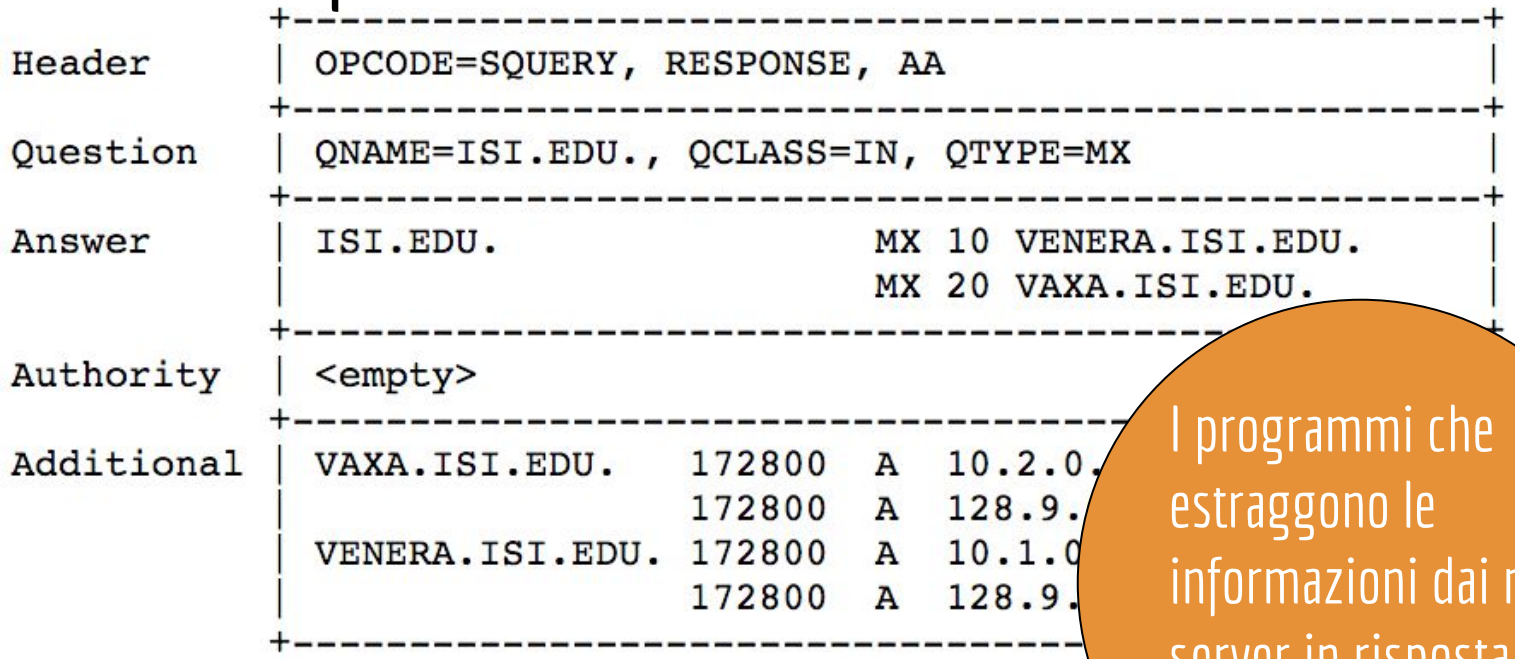
I tre componenti del DNS



I programmi che estraggono le informazioni dai name server in risposta alle richieste dei client

Resolvers

I tre componenti del DNS



I programmi che estraggono le informazioni dai name server in risposta alle richieste dei client

Resolvers

IN-ADDR.ARPA e IP6.ARPA

Speciali nomi a dominio per mappare gli IP (v4 e v6) agli host (NUMERO ⇒ NOME)

I dati dell'indirizzo 4 3 2 1
10. 2. 0. 52 possono essere rintracciati nel nome a dominio

1 2 3 4
52.0.2.10.IN-ADDR.ARPA.

I dati dell'indirizzo 2001:DB8::10:2:0:52 possono essere rintracciati nel nome a dominio

2.5.0.0.0.0.0.0.2.0.0.0.0.1.0.0.0.0.0.0.0.0.0.0.8.B.D.0.1.0.0.2.IP6.ARPA.

DNS query lab con *dig*

man dig

```
NAME
       dig - DNS lookup utility

SYNOPSIS
       dig [@server] [-b address] [-c class] [-f filename] [-k filename] [-m]
           [-p port#] [-q name] [-t type] [-x addr] [-y [hmac:]name:key] [-4]
           [-6] [name] [type] [class] [queryopt...]
```

dig @my-dns-server -c IN -t TXT mydomain.tld

dig mydomain.tld TXT

DNS query lab con *dig*

dig example.org A

```
; <<>> DiG 9.8.3-P1 <<>> example.org A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23618
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;example.org.                   IN      A

;; ANSWER SECTION:
example.org.            10800   IN      A       127.0.0.1

;; AUTHORITY SECTION:
example.org.            10800   IN      NS      example.org.

;; Query time: 45 msec
;; SERVER: 172.31.2.1#53(172.31.2.1)
;; WHEN: Sat Apr 23 20:28:54 2016
;; MSG SIZE  rcvd: 59
```

dig -x 127.0.0.1

```
; <<>> DiG 9.8.3-P1 <<>> -x 127.0.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54251
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; QUESTION SECTION:
;1.0.0.127.in-addr.arpa.        IN      PTR

;; ANSWER SECTION:
1.0.0.127.in-addr.arpa. 10800   IN      PTR     localhost.

;; AUTHORITY SECTION:
127.in-addr.arpa.       10800   IN      NS      localhost.
;; ADDITIONAL SECTION:
localhost.              10800   IN      A       127.0.0.1
localhost.              10800   IN      AAAA    ::1
;; Query time: 41 msec
;; SERVER: 172.31.2.1#53(172.31.2.1)
;; WHEN: Sat Apr 23 20:32:42 2016
;; MSG SIZE  rcvd: 121
```

DNSSEC

DNS Security Extensions

RFC

RFC 2535 Domain Name System Security Extensions
RFC 3833 A Threat Analysis of the Domain Name System
RFC 4033 DNS Security Introduction and Requirements (DNSSEC-bis)
RFC 4034 Resource Records for the DNS Security Extensions (DNSSEC-bis)
RFC 4035 Protocol Modifications for the DNS Security Extensions (DNSSEC-bis)
RFC 4398 Storing Certificates in the Domain Name System (DNS)
RFC 4470 Minimally Covering NSEC Records and DNSSEC On-line Signing
RFC 4509 Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)
RFC 5155 DNSSEC Hashed Authenticated Denial of Existence
RFC 6781 DNSSEC Operational Practices, Version 2

RESOURCE RECORDS

RRSIG (resource record signature)
DNSKEY
DS (delegation signer)
NSEC (next secure record)

DNS Security Extensions

Usare DNSViz a scopo didattico

Sandia National Laboratories

VERISIGN

DNS Security Extensions

RRset status

Secure (5)

- as59715.net/A
- as59715.net/AAAA
- as59715.net/MX
- as59715.net/NS
- as59715.net/SOA

DNSKEY/DS/NSEC status

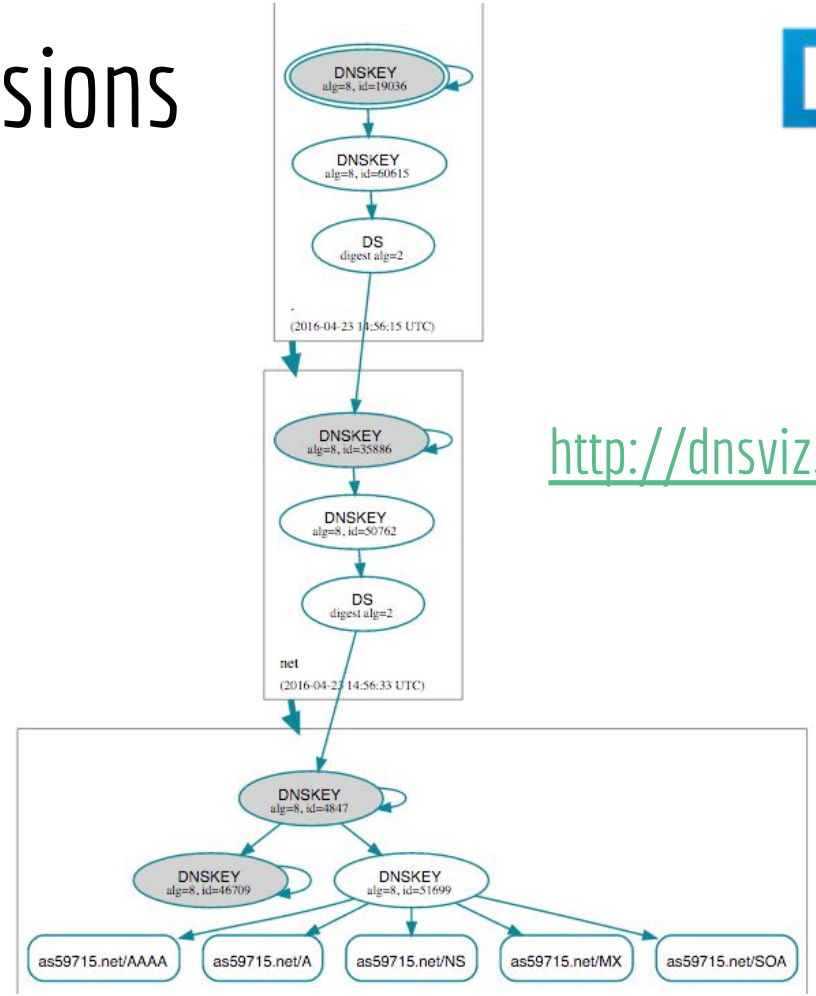
Secure (9)

- ./DNSKEY (alg 8, id 19036)
- ./DNSKEY (alg 8, id 60615)
- as59715.net/DNSKEY (alg 8, id 46709)
- as59715.net/DNSKEY (alg 8, id 4847)
- as59715.net/DNSKEY (alg 8, id 51699)
- as59715.net/DS (alg 8, id 4847)
- net/DNSKEY (alg 8, id 35886)
- net/DNSKEY (alg 8, id 50762)
- net/DS (alg 8, id 35886)

Delegation status

Secure (2)

- . to net
- net to as59715.net



DNSViz

http://dnsviz.net/d/as59715.net

Sandia National Laboratories

VERISIGN

DNS query lab con *dig +dnssec*

dig as59715.net SOA +dnssec

```
; <<>> DiG 9.8.1-P1 <<>> as59715.net SOA +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30953
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 7
;; QUESTION SECTION:
;as59715.net.                   IN      SOA
;; ANSWER SECTION:
as59715.net.            3454    IN      SOA     ns1.as59715.net. dnsmaster.as59715.net. 2016041691 86400 7200 604800 3600
as59715.net.            3454    IN      RRSIG   SOA 8 2 3600 20160502030035 20160425084750 51699 as59715.net.
DhIevNBDMIxQrCdUlO1ISK7/sNCjuNAfCLPcbh7CJDLNXulRPAhiJHZe vnI1TCYlrs5G01wyYjiIR4YN4+doPJIAzeggegWJ796hb/H69J78Q5rU
0J3pAX3ycr1Z7LOwLRktIQA7n8HQ3Hk6FoV0J6E8ZMj10AEUK2ISSFhy FKo=
;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Apr 25 10:14:50 2016
;; MSG SIZE  rcvd: 1043
```

DNS query lab con *dig +dnssec*

Salviamo l'àncora di fiducia

```
dig . DNSKEY | grep -Ev '^($|;)' > root.keys
```

DNS query lab con *dig +dnssec*

Verifichiamo la catena di fiducia, fino a risalire all'àncora:

dig +sigchase +trusted-key=./root.keys as59715.net. A

DNS query lab con dig +sigchase +trusted-key=./root.keys as59715.net. A

```
;; RRset to chase:
as59715.net.            84712   IN      A       185.5.200.86
;; RRSIG of the RRset to chase:
as59715.net.            84712   IN      RRSIG   A 8 2 86400 20160502040703 20160425064750 51699 as59715.net.
aU2wPgjkhA+CSb/eTH8rSN5cMnKkmkZDpynJAS2JBI74ujcFxzwBG6nH 5t1TB+pWTiIBx98HDKWE2fbx9igj5OMQvJEo1v/gxdRsXszh4No5Gg4g
HCWS5VUDX8uwDID+8zLuiF3NDNP5LxOvraKe/MfBfKBoyV/5CjnRqgkR gFw=
Launch a query to find a RRset of type DNSKEY for zone: as59715.net.
;; DNSKEYset that signs the RRset to chase:
as59715.net.            1912    IN      DNSKEY  257 3 8 AwEAAeNYZz0/uQ0FWA81uXKreLxJ1rj2KlLNKItg8T1/fzQDsPR6sy04
p5mlNad9B5p0UaPQbRMA4Dc1/mFd2mQwuinS9kAhFYAi0lE8YCAha0rP VHlOZwzI2G2d2iIG3sHcDzWLgyZBJenpheZDXOxmea9+4V4sWoADprVr
tRsnlPk13xfAdM7+Po+77CHMls7C5yjLz+IiHSGhtyURh0pdXeie0dmM ZO9V/pVeFfN4iGqbTro/Dexi/gZ6xXlyLXbfEDogxnlJgVQvEjh72GjS
Gy8Yo+3TVivq/qny4vsxSIoiZBNp68lB6m6GatukWFZrNPwOSmTIDoyt EDNBSpUJ0BM=
as59715.net.            1912    IN      DNSKEY  257 3 8 AwEAAe8MwOmRSTuyiEF0DbJdcnNrrP4ULRWDi/5jgdSALtlCmvCeAHWM
pASLLwfi85KzDjc1eIg7cHQgDdzZYo+Kh8z2Trk6AbRBqOPPN0J+MHk7 G7ruwRkSZT/dypkK2jE8bDusCUfcsWUbGzz8tsjARqJzmwED4iZIhlic
oFri7Dfqao7dO88EqWfG1T4JA4x5fizxrUpzsSm2JrM3rpjZBxE3vWXM 72W1PmU7A7Bvvkh5Pv6hyDLxdx7nHwas1OAX5aLLFPCSRPDVQ/kc+B0t
lyB2H4Rkm9TAJ+/UYgdkFuFTl/C/iW97AdXwCNinpUHo/zoR+BiBB48A IGAr4KiJoP0=
as59715.net.            1912    IN      DNSKEY  256 3 8 AwEAAcybp0wFl0yCOF+A7q9pbVMDhJrf0yRqzydF4X49w4R2rRO23ehY
uSRprsvMQSgCMRJ7t9zW2IMaRwmDZmeWjDZlYDLNFeljIzMIGg7xy1Ja yQ0iCW0JHgx+ebshwol4WvjQFyhYcdgWZMIgboMUmCgO+95z4wUQ1Eyh 8UblR2u7
```

DNS query lab con dig +sigchase +trusted-key=./root.keys as59715.net. A

```
;; RRSIG of the DNSKEYset that signs the RRset to chase:
as59715.net.            1912    IN      RRSIG   DNSKEY 8 2 3600 20160429231648 20160422104750 4847 as59715.net.
oDWYrIdpQaLF4wdYyXSMsn0zB3FkhDYWmsz2tgTdsdiWU2Qjoijnf846 1bN/uiEpSVoVbybq9y6dkprAkD4Of8GHynw18tBb+4CB3rEO2NCj7GPM
ujdhwDt3hBocNe9IHu5snTgX3qIAQAW72Mxw6GWPq8pneZ9rSWpm3v4F ZOO5nN8Q+iNxpOTuHoW9EbosN8P9Se3HIl8+2YtTWDEzumqkOTxa2AmO
E21if7zb3/2zqExb3eWcPX7cQVWpTjzsGmBPdMQTDKTNOizD4Vrot/N2 Z2VdWEZ7n9srX/SpRjJve1cYF4ExUwKitho0WdSI0AwIVeI7Fse+daac d5LC8Q==
as59715.net.            1912    IN      RRSIG   DNSKEY 8 2 3600 20160429231648 20160422104750 46709 as59715.net.
ehMBH+d3hqRIoNtnpfsFmCCtEYiF8whwW2c/4MMEuUxhXKYFwLb0sxy6 1jTBnaLW3mGNUDebKta/OpMjECMPVHvZPBmj3GQBHgxQBvvYDpkafwJG
/9RJ+Wvrfs/+vch7PvjVhYxAxibDnVvI81V7/Z+EyFen+kgN5Fv5Rsz1 XFlysHG3T8kiFihzYl3nUbd1Rk3Yzx/Ngv5CgtkW6sfoBUBaxU+JWJSC
I1NSE8A3MdWJMpxd3Br7AsfIbiGI+0U5tOstnolf6/QLTIU8Z+IpkPqB DfmB+vtSW8VlgR5enRuSBm5YWNguz/50gH1D4ja4wsxRtiuXCcKr/Yl+ ugwGrg==

Launch a query to find a RRset of type DS for zone: as59715.net.
;; DSset of the DNSKEYset
as59715.net.            42554   IN      DS      4847 8 2 69A705E2835DCAE42BDB4C82B2E7260ABF918C164954ECA329AEBB90 10110352

;; RRSIG of the DSset of the DNSKEYset
as59715.net.            42554   IN      RRSIG   DS 8 2 86400 20160429051243 20160422040243 50762 net.
ac7vB9F3G325wuOF52YB7Jf+9r0UHGkDgHzYQeOIaOD8Op57gLhVcae1 Ie0wV/zac9OrTWfEG2IyLG1RxbKLGnrrtpGrrXiMt2/Rp8W4G1P2MRIS
5G4teAAEkwn2ucMRVr5oIbLv8Ms2LLzDPQIZqITRj+tN8gFUX+1OIJUX 78s=
```

DNS query lab con dig +sigchase +trusted-key=./root.keys as59715.net. A

```
;; WE HAVE MATERIAL, WE NOW DO VALIDATION
;; VERIFYING A RRset for as59715.net. with DNSKEY:51699: success
;; OK We found DNSKEY (or more) to validate the RRset
;; Now, we are going to validate this DNSKEY by the DS
;; OK a DS valids a DNSKEY in the RRset
;; Now verify that this DNSKEY validates the DNSKEY RRset
;; VERIFYING DNSKEY RRset for as59715.net. with DNSKEY:4847: success
;; OK this DNSKEY (validated by the DS) validates the RRset of the DNSKEYs, thus the DNSKEY validates the RRset
;; Now, we want to validate the DS :  recursive call
Launch a query to find a RRset of type DNSKEY for zone: net.
;; DNSKEYset that signs the RRset to chase:
net.                    10829   IN      DNSKEY  257 3 8 AQOYBnzqWXIEj6mlgXg4LWC0HP2n8eK8XqgHlmJ/69iuIHsa1TrHDG6T
c0ra/pyeGKwH0nKZhTmXSuUFGh9BCNiwVDuyyb6OBGy2Nte9Kr8NwWg4 q+zhSo0f4D+gC9dEzg0yFdwT0DKEvmNPt0K4jbQDS4Yimb+uPKuF6yie
WWrPYYCrv8C9KC8JMze2uT6NuWBfsI2fDUoV4I65qMww06D7n+p7Rbdw WkAZ0fA63mXVXBZF6kpDtsYD7SUB9jhhfLQE/r85bvg3FaSs5Wi2BaqN
06SzGWI1DHu7axthIOeHwg00zxIhTpoYCH0ldoQz+S65zWYi/fRJiyLS Bb6JZOvn
net.                    10829   IN      DNSKEY  256 3 8 AQPNMFqRLYVsvz7L1y7athCoAHynoJiOVUijHAlQ2o70ZTUsQb0RJsAK
QlFztuClkFMzweDRIochZ7y7JWCLqUzGAmtbT2T7duYQk+eGHqbz4Fmu aZEMDuvQ1zkFQFYbO4vuWZ2IFESXjZkYhzmkkEQYpjPoF3yzUGnud6w5 QksP0Q==
```

DNS query lab con dig +sigchase +trusted-key=./root.keys as59715.net. A

```
;; RRSIG of the DNSKEYset that signs the RRset to chase:
net.                    10829   IN      RRSIG   DNSKEY 8 1 86400 20160430163857 20160415163357 35886 net.
PvD6FwoWU6FuIVBFYRMQgs/5qXWQmeToydXav0/NTLDegTPbPrCBA+Mv hbyTUfDsvPUYDLX5NDj7ouJfy0kFRGkmRPd0HcD/dc3uz6PMCiGPutKm
Prys6VkTDYfZ4nEPHXHwSVfHnFq++Z5K/LbELjRJ92h/lJJzKLwRnxs+ WzMmGvVD9FjkMIQwVcSjKEZuQNpzwojV01NbUQHz7mbLcHMSsiTasB3q
vV8rYIotgUNIZ0AQNYhgvJ3xUJpNDA9CPvOmVbs5SJjBqjYx0ksdSni6 ZQLfUYbnSck5SlpK+PEqlAUgh+QZRaHVtjefCYmVQ5EWv+2rWLsuocVP s6wHhA==

Launch a query to find a RRset of type DS for zone: net.
;; DSset of the DNSKEYset
net.                    10829   IN      DS      35886 8 2 7862B27F5F516EBE19680444D4CE5E762981931842C465F00236401D 8BD973EE

;; RRSIG of the DSset of the DNSKEYset
net.                    10829   IN      RRSIG   DS 8 1 86400 20160504050000 20160424040000 60615 .
eENolj/7cojfwxWjbGQ81FSS9nnyXia9Q+w1nxtPP3jC3Mprhb+VBaKr LzZ58uDbagix79FlWUEz/8bHkDg23e7qBkt53dtKxoOPBjpMI8xjHhEy
IKt9kwKTdj3aLGsr6oabkQmLZRlfBpev1rm5I1hd1hoDilRVuvM3zySr 1qA=
```

DNS query lab con dig +sigchase +trusted-key=./root.keys as59715.net. A

```
;; WE HAVE MATERIAL, WE NOW DO VALIDATION
;; VERIFYING DS RRset for as59715.net. with DNSKEY:50762: success
;; OK We found DNSKEY (or more) to validate the RRset
;; Now, we are going to validate this DNSKEY by the DS
;; OK a DS valids a DNSKEY in the RRset
;; Now verify that this DNSKEY validates the DNSKEY RRset
;; VERIFYING DNSKEY RRset for net. with DNSKEY:35886: success
;; OK this DNSKEY (validated by the DS) validates the RRset of the DNSKEYs, thus the DNSKEY validates the RRset
;; Now, we want to validate the DS :  recursive call
Launch a query to find a RRset of type DNSKEY for zone: .
;; DNSKEYset that signs the RRset to chase:
.                       169159  IN      DNSKEY  256 3 8 AwEAAarQO0FTE/I6LEKFlZIlJIwXuLGd3q5d8S8NH+ntOeIMN81A5wAI
18g3u9w/esNkThwgXTEa2mX1iOPdTcI3yRIeAExxF22IEU2E0GKY2XdY r/BxP5fojJAPRgtEGDI72NSwSnD2/a8uPNirAJZoab36Hlw41QxEI7bm Co0280mt
.                       169159  IN      DNSKEY  257 3 8 AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dIzEheX7ICJBBtuA6G3LQpz W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYI7OyQdXfZ57relS
Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq QxA+Uk1ihz0=
```

DNS query lab con dig +sigchase +trusted-key=./root.keys as59715.net. A

```
;; RRSIG of the DNSKEYset that signs the RRset to chase:
.                       169159  IN      RRSIG   DNSKEY 8 0 172800 20160505235959 20160421000000 19036 .
SIEw2yBGjB72FvKkavke5w90pBlx7YuKqaEzchZBjWAE6BybMQKT2G5C Is/R6KAjG9sPCQu5bsu/GAjP2YhCVyVtVZ7x0ngqlbwfwQCuo2Xq+aym
nszrhN0jijmb7sqd9Ww7rFigAkyOaNWGAikVgeuCNvwlhcfVrr2QruO0 z2C4P/ULUyqrnKO3Mr9vK2Z1PiBbO2PtRbFOn3xIkcy3WV+1QLS5Xox0
S3ZZZGj6ICu3v/LbrsuWejmXSvZaMfQt1leo3v4dmhYMzD14xsyx6qb5 2VYDgajsDuhvV0zCavgAoNLwchWhHccagnuufG3YIkbF8rMr1m6f1D/m 5mgXJA==

Launch a query to find a RRset of type DS for zone: .
;; NO ANSWERS: no more
;; WARNING There is no DS for the zone: .

;; WE HAVE MATERIAL, WE NOW DO VALIDATION
;; VERIFYING DS RRset for net. with DNSKEY:60615: success
;; OK We found DNSKEY (or more) to validate the RRset
;; Ok, find a Trusted Key in the DNSKEY RRset: 60615
;; Ok, find a Trusted Key in the DNSKEY RRset: 19036
;; VERIFYING DNSKEY RRset for . with DNSKEY:19036: success

;; Ok this DNSKEY is a Trusted Key, DNSSEC validation is ok: SUCCESS
```

YETI DNS Project

Research topics:

- IPv6-only operation
- DNSSEC key rollover
- Renumbering issues
- Scalability issues
- Multiple zone file signers

join us

www.yeti-dns.org

Questions?