

APNIC eLearning: DNS Security

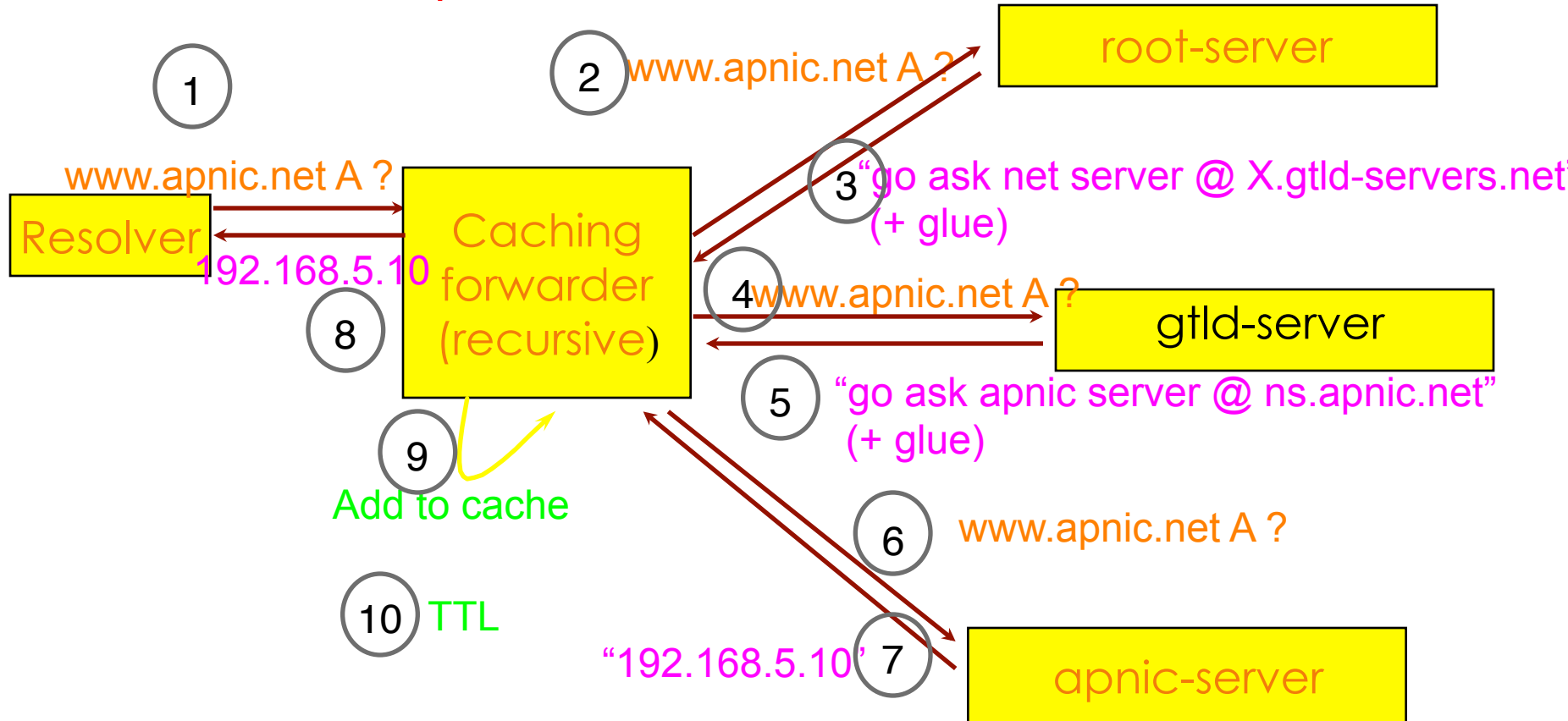
Contact: training@apnic.net

Overview

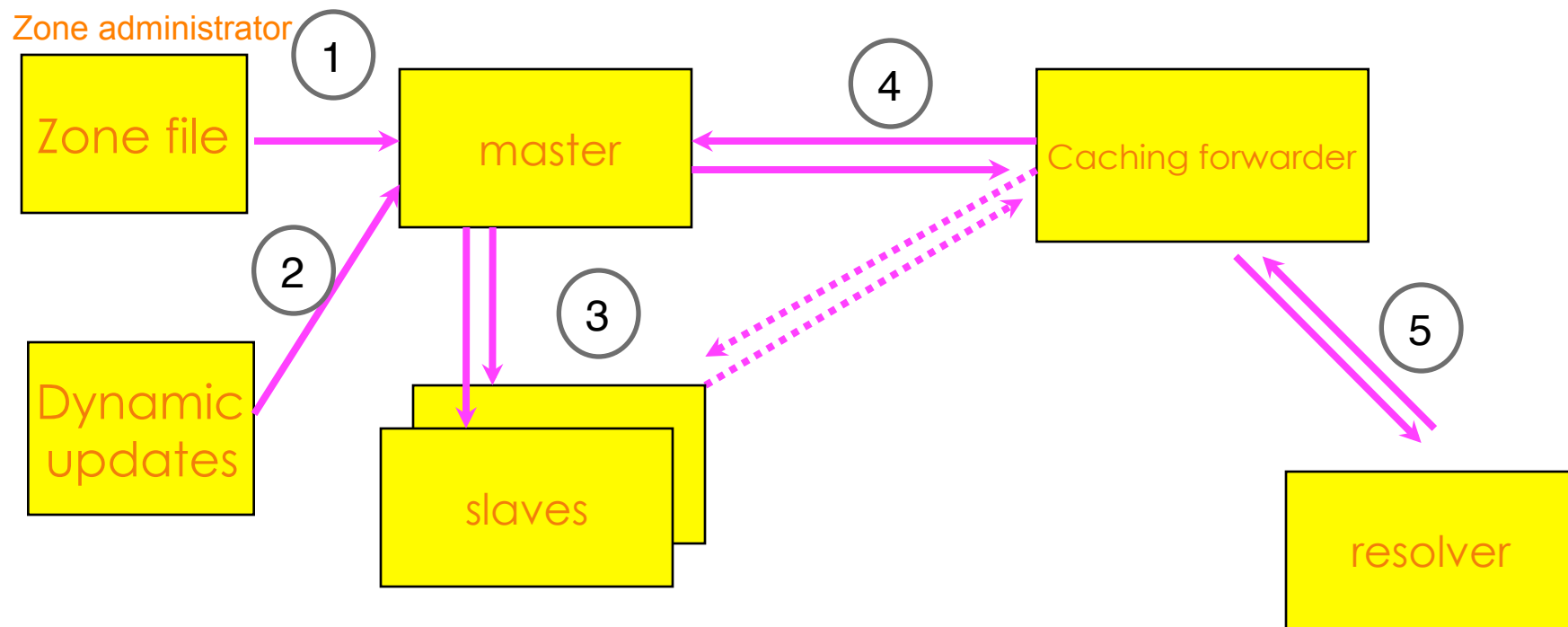
- How DNS Works
- DNS Vulnerabilities
- Securing the Nameservers
- Transaction Signature (TSIG)
- DNS Security Extensions (DNSSEC)
- DNSSEC New Resource Records
- Signing Zones

Overview: How DNS Works

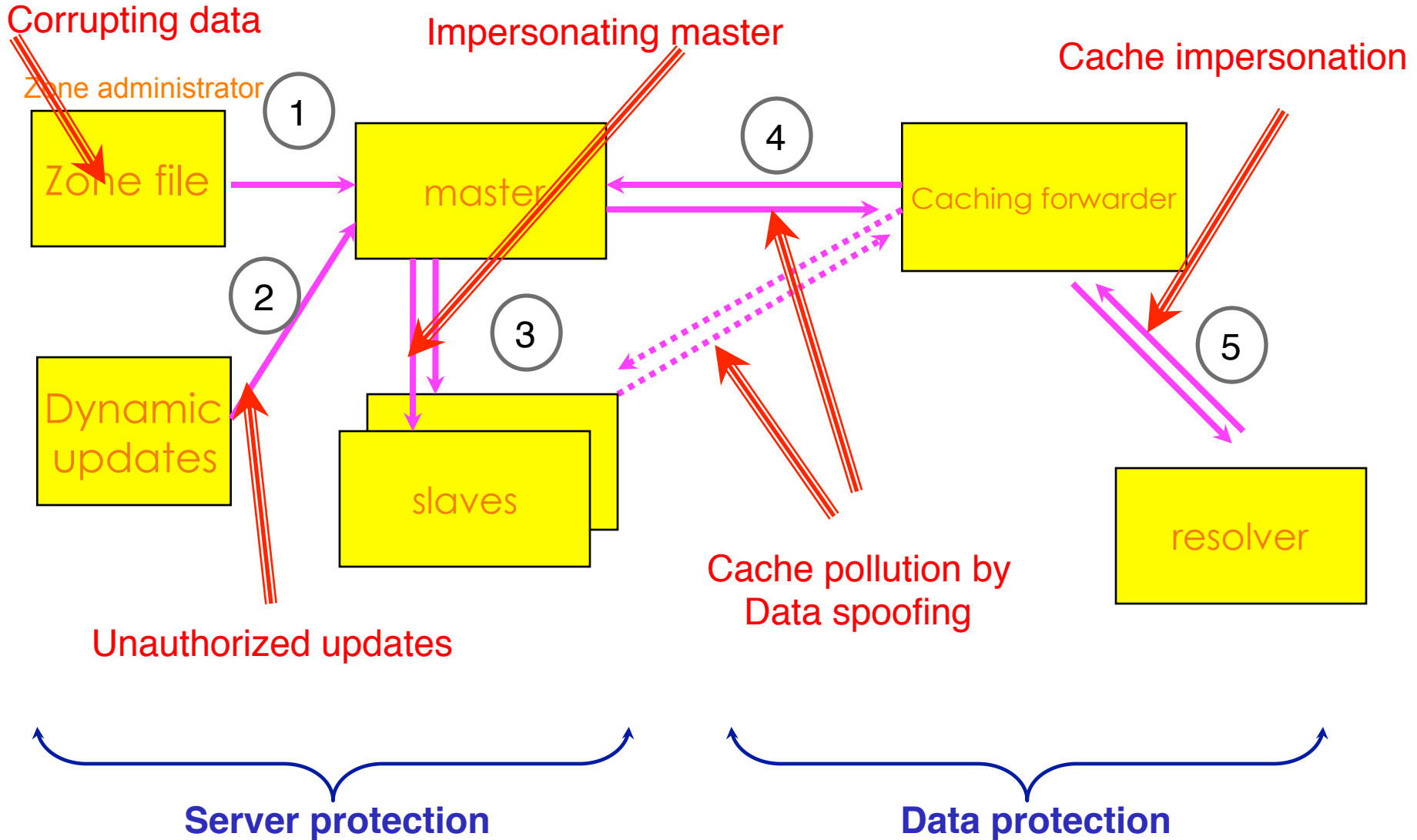
Question: **www.apnic.net A**



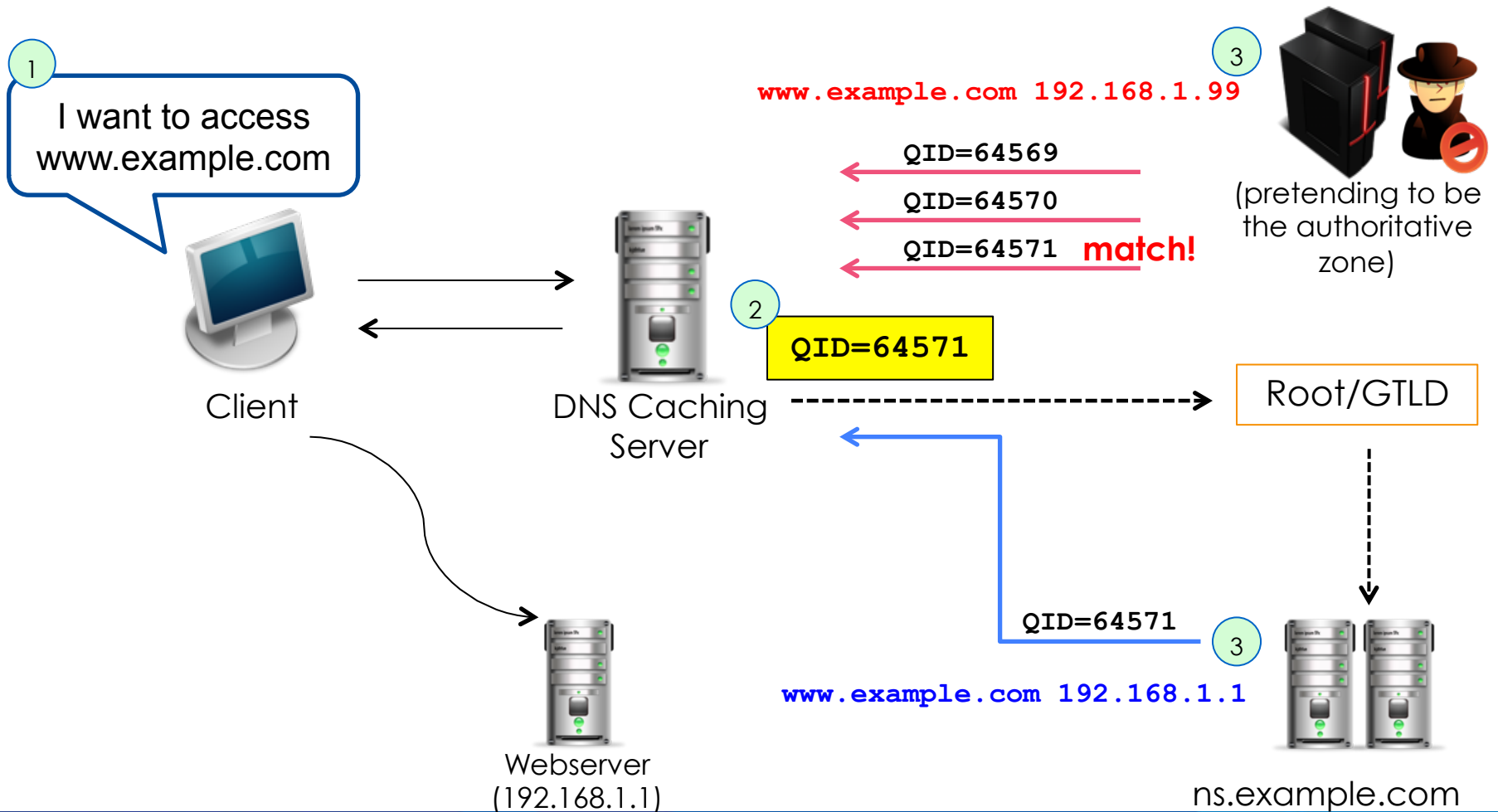
DNS Vulnerabilities



DNS Vulnerabilities



DNS Cache Poisoning



RFC 4033: DNS Security Introduction and Requirements

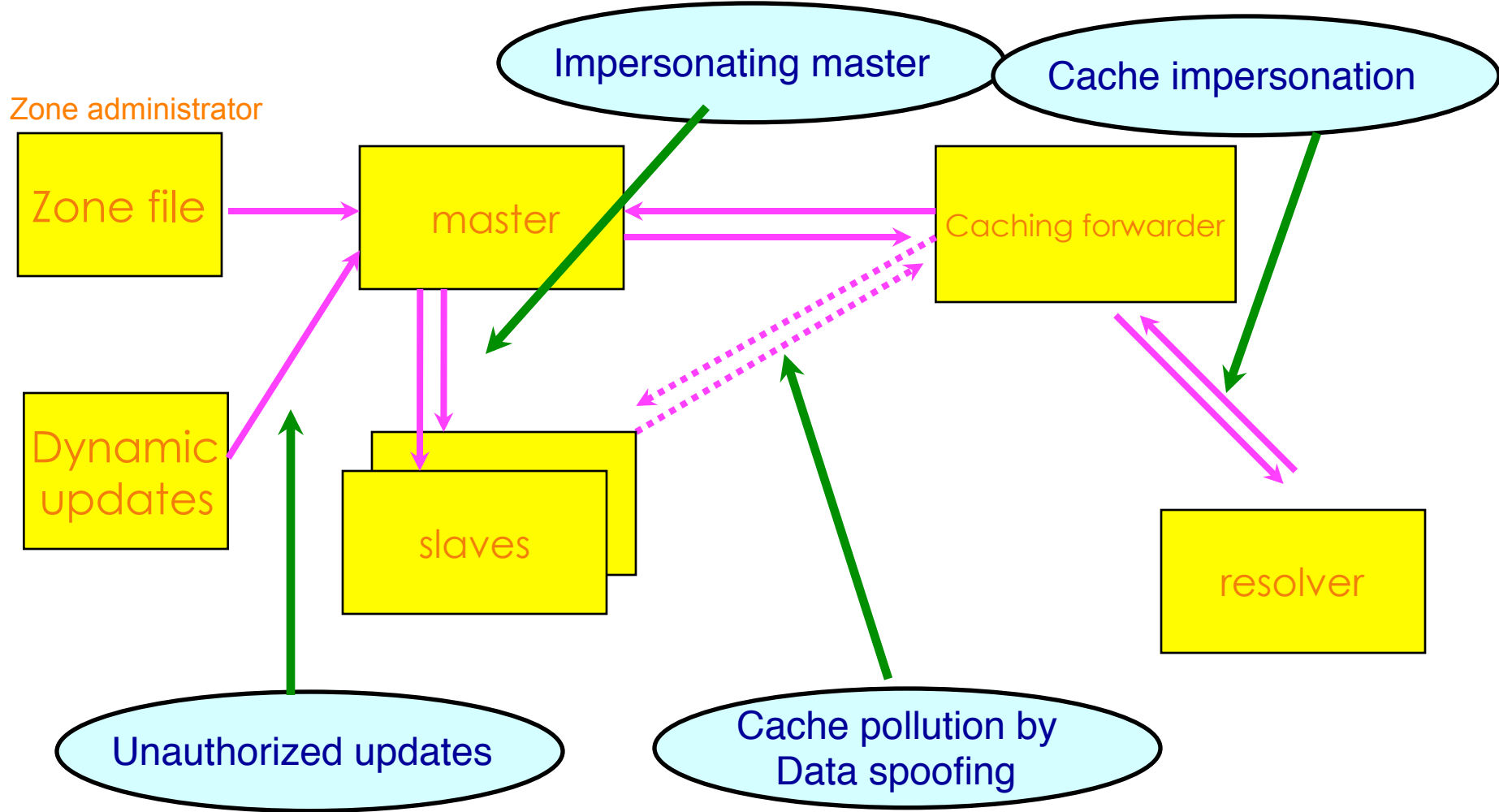
Securing the Nameserver

- Run the most recent version of the DNS software
 - Bind 9.9.1 or Unbound 1.4.16
 - Apply the latest patches
- Hide version
- Restrict queries
 - `Allow-query { acl_match_list; };`
- Prevent unauthorized zone transfers
 - `Allow-transfer { acl_match_list; };`
- Run BIND with the least privilege (use `chroot`)
- Randomize source ports
 - don't use `query-source` option
- Secure the box
- Use TSIG and DNSSEC

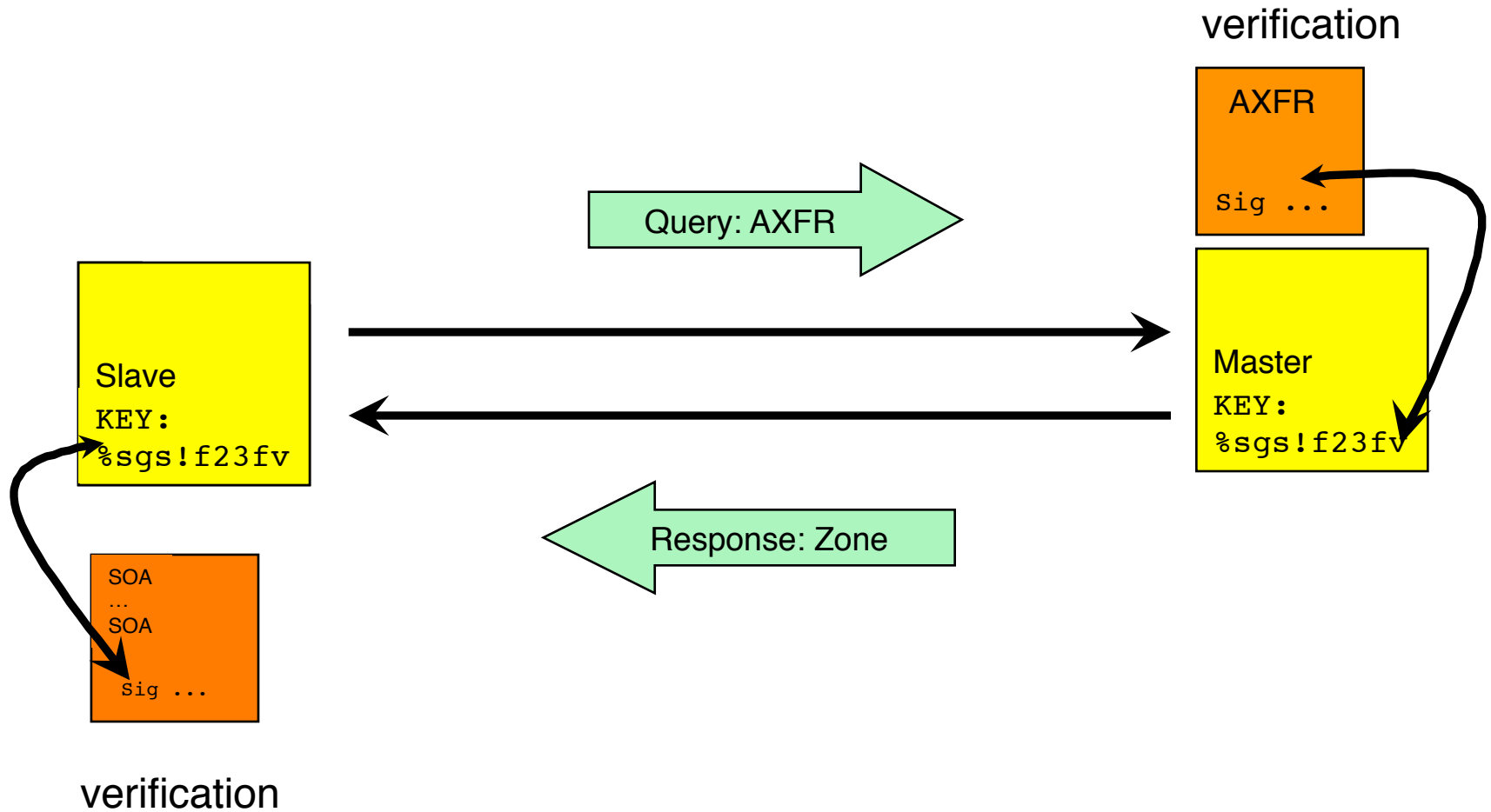
Transaction Signature (TSIG)

- A mechanism for protecting a message from a primary to secondary and vice versa (i.e. transactions)
- A keyed-hash is applied (like a digital signature) so recipient can verify message
 - DNS question or answer & the timestamp
 - Based on a shared secret - both sender and receiver are configured with it
- RFC 2845

TSIG Protected Vulnerabilities



TSIG Example



TSIG Steps

- Generate secret
 - `dnssec-keygen -a <algorithm> -b <bits> -n host <name of the key>`
- Communicate secret
 - Transfer the key securely (ex. SSH/SCP)
- Configure the servers
 - Edit configuration file for primary and secondary
- Test
 - `dig @<server> <zone> AXFR -k <TSIG keyfile>`

TSIG Configuration – named.conf

Primary server 10.33.40.46

```
key ns1-ns2.pcx. net {  
    algorithm hmac-md5;  
    secret "APlaceToBe";  
};  
server 10.33.50.35 {  
    keys {ns1-ns2.pcx.net};  
};  
  
allow-transfer {  
    key ns1-ns2.pcx.net ;};
```

Secondary server 10.33.50.35

```
key ns1-ns2.pcx.net {  
    algorithm hmac-md5;  
    secret "APlaceToBe";  
};  
server 10.33.40.46 {  
    keys {ns1-ns2.pcx.net};  
};  
zone "my.zone.test." {  
    type slave;  
    file "myzone.backup";  
    masters  
        {10.33.40.46};};
```

You can save this in a file and refer to it in the config file (named.conf) using 'include' statement:

```
include "/var/named/master/tsig-key-ns1-ns2";
```

TSIG Testing - dig

- You can use dig to check TSIG configuration

```
dig @<server> <zone> AXFR -k <TSIG keyfile>
```

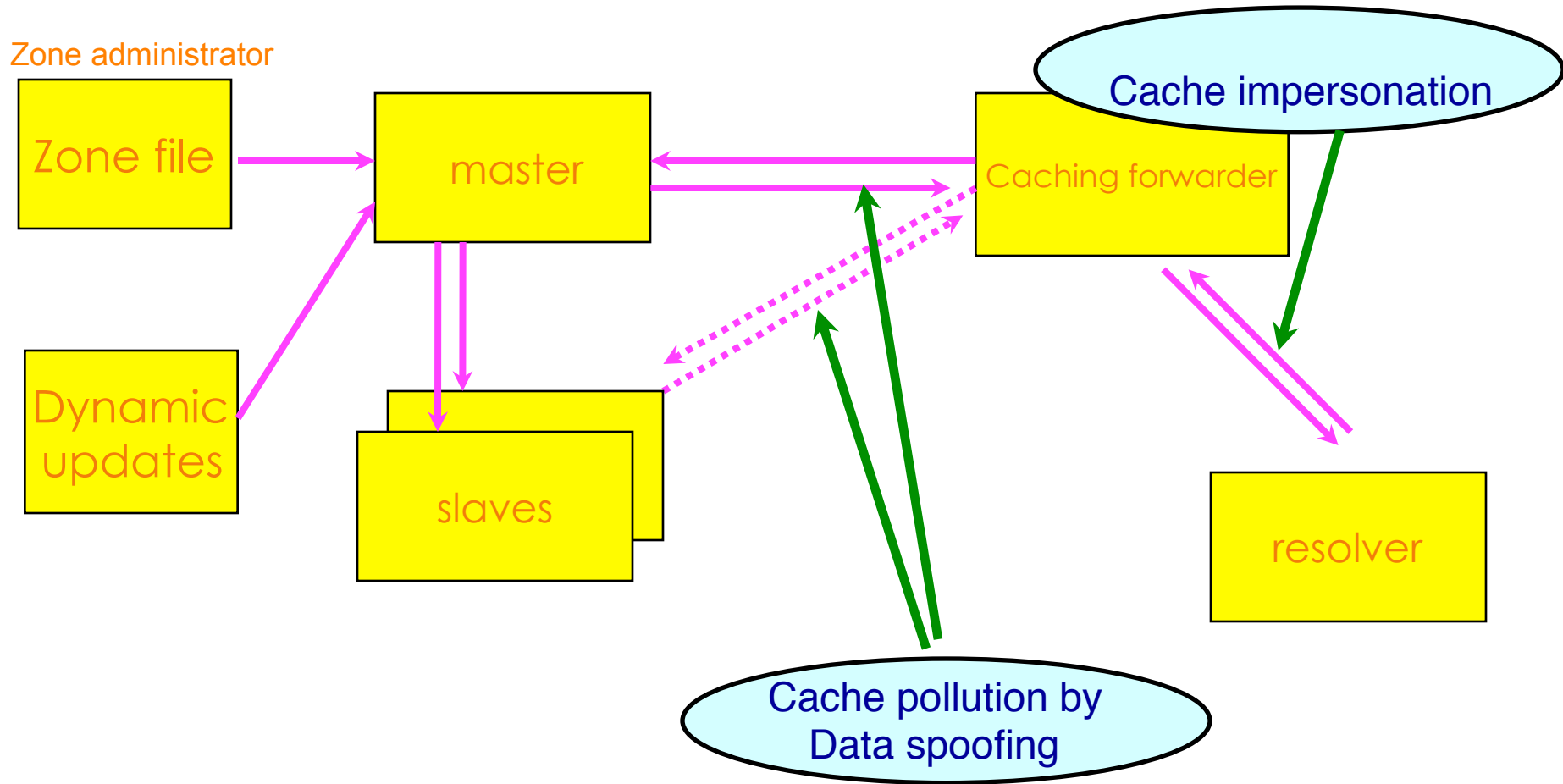
```
$ dig @127.0.0.1 example.net AXFR \  
-k Kns1-ns2.pcx.net.+157+15921.key
```

- A wrong key will give “Transfer failed” and on the server the security-category will log this.
- Note: TSIG is time-sensitive

DNS Security Extensions (DNSSEC)

- Protects the integrity of data in the DNS by establishing a chain of trust
- A form of digitally signing the data to attest its validity
- RFC 4033, 4034, 4035
- DNSKEY/RRSIG/NSEC: provides mechanisms to establish authenticity and integrity of data
- DS: provides a mechanism to delegate trust to public keys of third parties

Vulnerabilities protected by DNSSEC



DNSSEC New Resource Records

- 3 Public key crypto related RRs
 - RRSIG = Signature over RRset made using private key
 - DNSKEY = Public key, needed for verifying a RRSIG
 - DS = Delegation Signer; 'Pointer' for building chains of authentication
- One RR for internal consistency
 - NSEC = Next Secure; indicates which name is the next one in the zone and which typecodes are available for the current name
 - authenticated non-existence of data

Types of Keys

- Zone Signing Key (ZSK)
 - Sign the RRsets within the zone
 - Public key of ZSK is defined by a DNSKEY RR
- Key Signing Key (KSK)
 - Signed the keys which includes ZSK and KSK and may also be used outside the zone
- Trusted anchor in a security aware server
- Part of the chain of trust by a parent name server
- Using a single key or both keys is an operational choice (RFC allows both methods)

DNSSEC - Setting up a Secure Zone

- Enable DNSSEC in the configuration file (named.conf)
 - `dnssec-enable yes; dnssec-validation yes;`
- Create key pairs (KSK and ZSK)
 - `dnssec-keygen -a rsasha1 -b 1024 -n zone champika.net`
- Publish your public key
- Signing the zone
- Update the config file
 - Modify the zone statement, replace with the signed zone file
- Test with dig

Signing the Zone

- `dnssec-signzone -o champika.net db.champika.net Kchampika.net.+005+33633`
- Once you sign the zone a file with a .signed extension will be created
 - `db.champika.net.signed`
- Note that only authoritative records are signed NS records for the zone itself are signed
 - NS records for delegations are not signed
 - DS RRs are signed!
 - Glue is not signed
- Difference in the file size
 - `db.champika.net` vs. `db.champika.net.signed`

Testing with dig: an example

**dig @localhost www.champika.net
+dnssec +multiline**

```
bash-3.2# dig @localhost www.champika.net +dnssec +multiline
; <<> DiG 9.6.0-APPLE-P2 <<> @localhost www.champika.net +dnssec +multiline
; (3 servers found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 37425
;; Flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.champika.net.      IN A

;; ANSWER SECTION:
www.champika.net.      86400 IN A 192.168.1.2
www.champika.net.      86400 IN RRSIG A 5 3 86400 20091123163643 (
                        20091024163643 22827 champika.net.
                        Eyp1IVyQyYBLK0X2u/LT1+40xjBomXzLrcdwSEngioMb
                        pGyDWDLzP+FTbE3QCfBMLNDt2AGoYctylcfY4li9sHkw
                        fue6hTQTsm0LhisBkVKQBy6ZD5oGiJQgaIkBGmLtVvPh
                        jGj8Z1UhbWkcGGK13doAa+5X8mx6MXNCudiNWeg= )

;; AUTHORITY SECTION:
champika.net.          86400 IN NS ns.champika.net.
champika.net.          86400 IN RRSIG NS 5 2 86400 20091123163643 (
                        20091024163643 22827 champika.net.
                        CZsPewlhPWpYt18wPh09Qhd6pWt0If2mLVshviGKq4no
                        ISNVoijmX0LyIns+o3DZz/2+TtwoQCRFLbfI99YMS3fx
                        BHGYqFDeGItYVx3oBpmTuAtMu2+od5WFS+LClsJsEP/N
                        QvUDgtWjrj8+Z0wVVj8aLe+I51h29ek7Mzk7+P4E= )

;; ADDITIONAL SECTION:
ns.champika.net.       86400 IN A 192.168.1.1
ns.champika.net.       86400 IN RRSIG A 5 3 86400 20091123163643 (
                        20091024163643 22827 champika.net.
                        eTP05c4GscnoC9V5sR6vgDo02WgCr1T5arU7YZhWctXI
                        vkmUini+wgUwqW6xezFB/Eu4J69bMnpQoX2zWUDtLUCM
                        +FVLsFx4Bbt+BjPEJKV03g9vv6IdkR/pxyE1kJWJWmI
                        tR49P2dywlzqqTyvnj3F1yuFRTLHhJvfvc+n8w= )

;; Query time: 3 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Oct 25 03:40:38 2009
;; MSG SIZE rcvd: 610
```

Questions

- Please remember to fill out the feedback form
 - `<survey-link>`
- Slide handouts will be available after completing the survey



APNIC Helpdesk Chat



Your IP address:
2001:dc0:a000:4:595f:4f90:654f:402c

Contact us | Press | Jobs | Site map

Home Services Community Events Publications About us

Services

Services APNIC provides

- > Registration services
- > Informing the community
- > Routing Registry
- > Resource certification
- > Training & education
- > Policy development
- ✓ Helpdesk
 - Using VoIP

- > Apply for resources
- > Become a Member
- > Make a payment
- > Manage Internet resources
- > Helpdesk

Helpdesk

Monday - Friday
09:00 to 21:00 (UTC +10)

 **Email**
helpdesk@apnic.net

 **Phone**
+61 7 3858 3188

 **VoIP**
helpdesk@voip.apnic.net

 **Fax**
+ 61 7 3858 3199

Multi-language phone support
Bahasa Indonesia, Bengali, Cantonese, English, Filipino (Tagalog), Hindi, and Mandarin.

 **APNIC Live Chat Online**
Click here to chat

Frequently asked questions

Request Live! Support

livehelp.apnic.net/request.php?l=apnplive&x=1&deptid=1&pa...

APNIC Helpdesk Chat

Welcome to our Live Chat.

Name

Email

What is your question?

Chat

Powered by PHP Live! v3.3 © OSI Codes Inc.

- > A-Z Glossary
- > Contact APNIC

Helpdesk queries

APNIC's Member Services
Helpdesk can assist you receive faster responses for:

- Status of requests
- Membership enquiries
- Billing issues
- Database enquiries

Existing members
Please use [MyAPNIC](#) to apply for resources.

Public holidays

APNIC offices and Helpdesk
are closed for the following

Thank you!

End of Session