Inline Signing in BIND 9.9

Internet Systems Consortium

January 11, 2012

About the Presenters

Michael Graff

BIND 9 Engineering Manager

mgraff@isc.org

@skandragon

Larissa Shapiro

ISC Product Manager

larissas@isc.org

@larissashapiro

Agenda

- Introductions & Logistics
- ISC Overview
- BIND 9.9: Inline Signing
- ISC Services and DNSSEC
- Questions

Logistics

- Attendees are muted but please feel free to ask questions using the Q & A panel or raise your “hand” to be called on to speak

- Questions will be answered at several points in the webinar as well as at the end of the session.

- An archive of this presentation and the slides will be available within three business days at:

http://www.isc.org/webinars

ISC in a Nutshell

Forum

- BIND
- BIND 10 Working Group
- DHCP
- AFTR / PCP
- SRF
- Open Source Routing

... and more to come.

Professional Services

- Consulting
- Training
- Software Support Services
- Custom Software Development
- F-Root Corporate Node
- DNS SNS-Com
- Full version of Domain Survey

Public Benefit Services

- DNS F-Root
- DNS Secondary Server Resiliency (SNS-PB)
- Hosted@ - hosting a range of open source projects
- Free Domain Survey Report
- Participation in IETF, RIPE WG, ICANN, ARIN, ISOC, UKNOF, etc

Empowerment

- Standards Driver - with first implementation of standards based code.
- Policy Meetings - Empowering Spheres of Influence
- Operational Security - Pioneering new approaches to safe guard the Internet (OPSEC-Trust)
- Operations Meetings Empowerment (APRICOT, AFNOG, NANOG, etc)
- Research (DNS OARC)

What is Inline Signing?

- A BIND 9.9 server reads unsigned data, and signs it automatically
- The source of the data can be another server (zone transfer) or a disk file
- Probably usable by nearly everyone
  - Eliminates using `dnssec-signzone`
  - Simplifies DNSSEC deployment
- It does not maintain keys, however

Inline Signing Benefits

- Deploying DNSSEC
- Use an IPAM or other source
- Minimize cost
- Minimize operational changes
- Parallel production and testbed
- Selective exposure

Any questions?

Need help with ISC products?

http://kb.isc.org -- ISC Knowledge Base

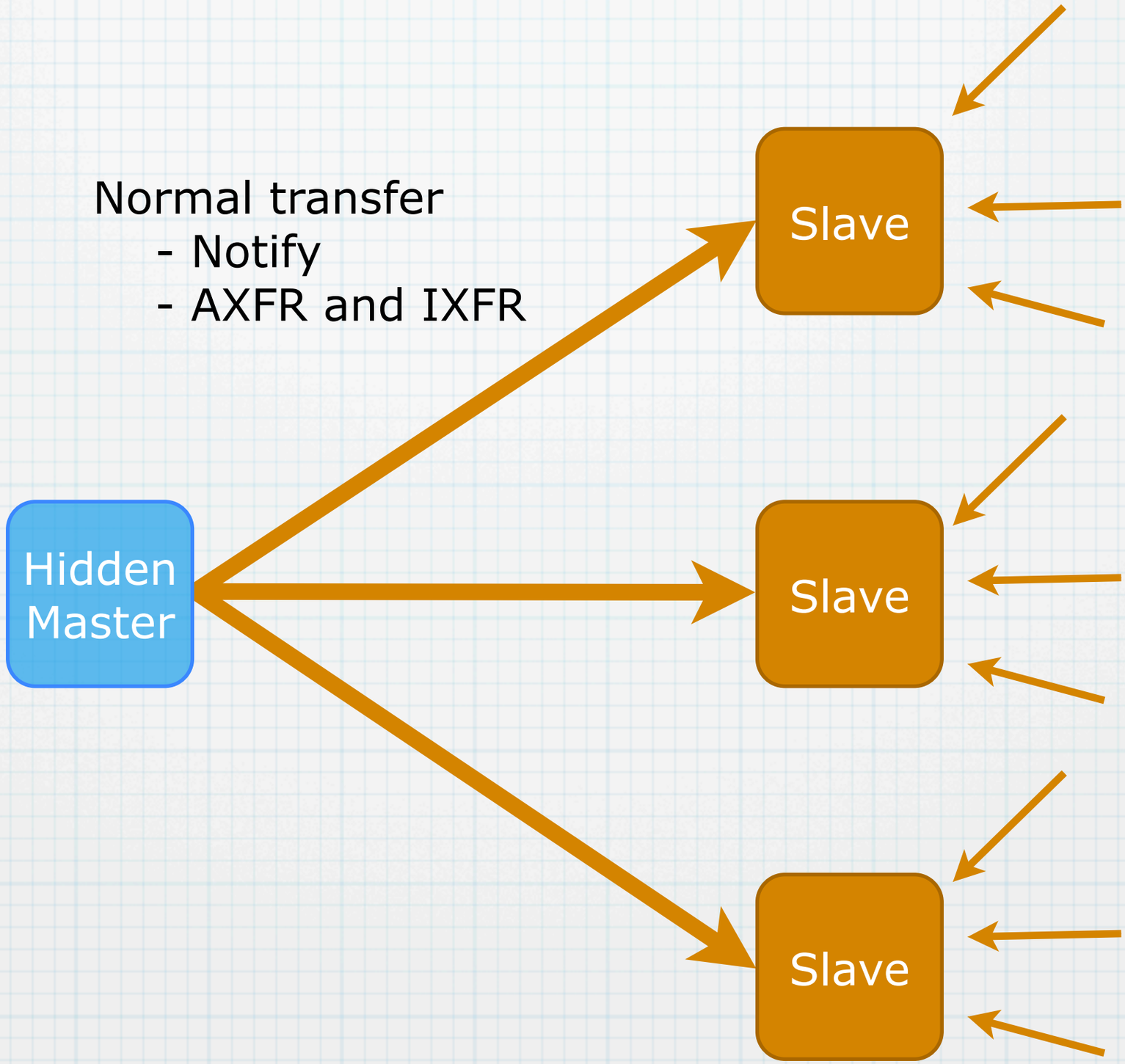
email lists (bind-users, etc)

Hidden Master

- Hidden masters are very common.
- Master server receives updates, and notifies slaves of changes.
- Slave transfer from the master using AXFR and IXFR.
- The master itself is not queried by resolvers.

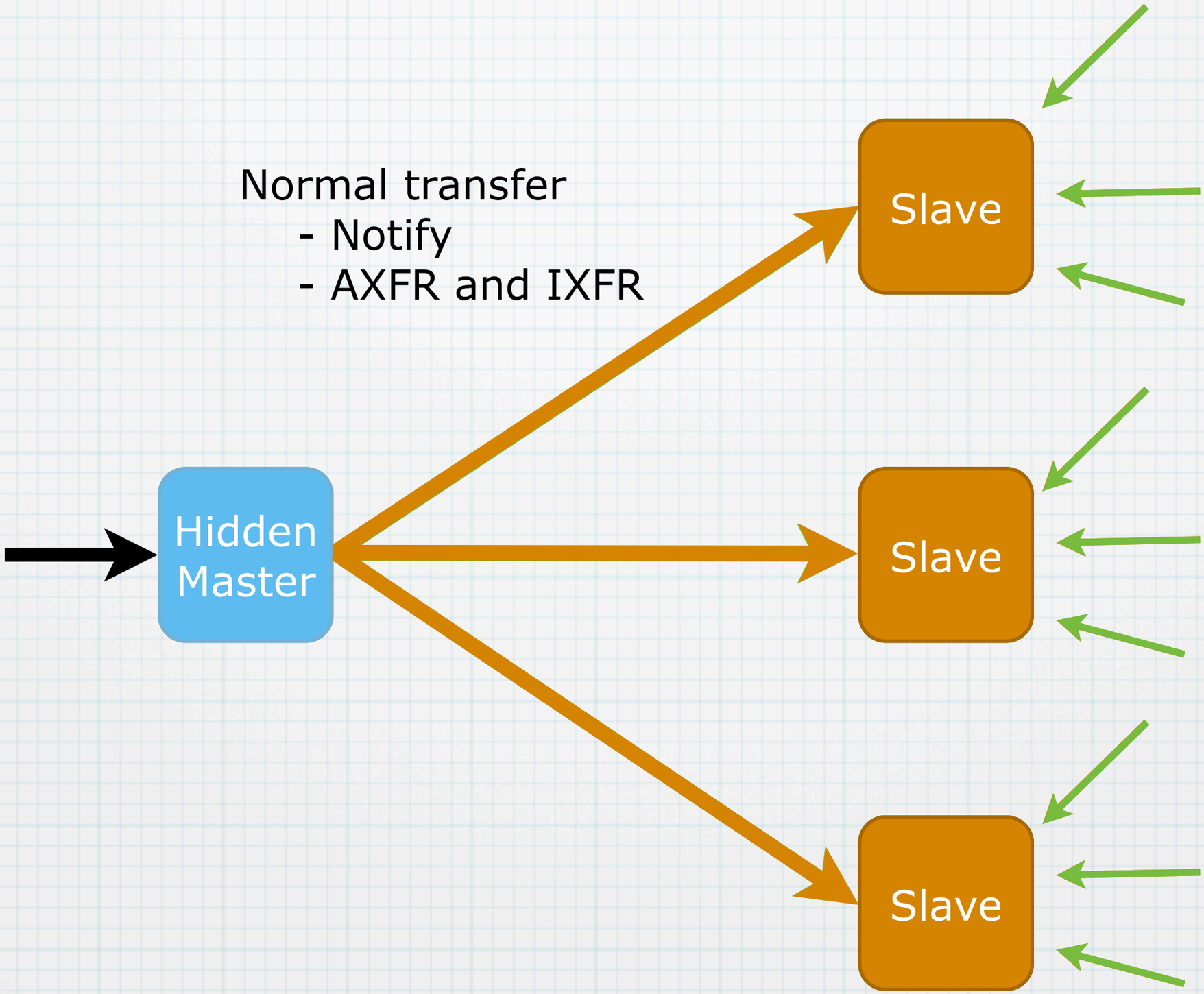
Hidden Master

Normal transfer
- Notify
- AXFR and IXFR



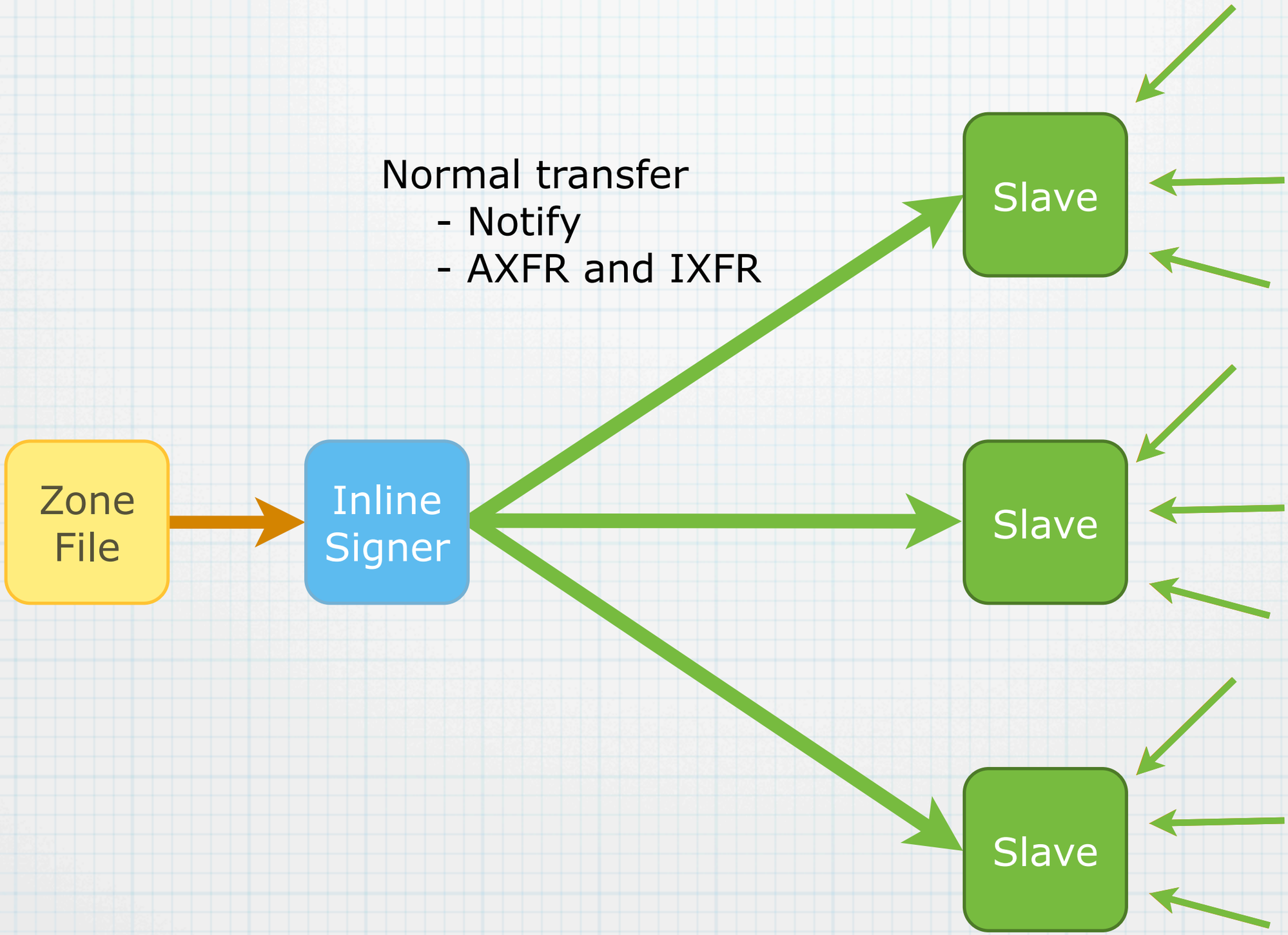
Inline Signing (slave model)

Normal transfer
- Notify
- AXFR and IXFR



Inline Signing (file model)

Normal transfer
- Notify
- AXFR and IXFR



Any questions?

Not using a hidden master?

Doing something special?

Contact ISC for support and consulting

sales@isc.org

Configuration

* So, how do we configure this stuff?

* Two models
  * Slave model
  * File model

Configuration

Enable Inline-Signing

```
inline-signing yes;
```

Enable DNSSEC automatic signing

```
auto-dnssec maintain;
```

Set key directory (optional)

```
key-directory "keys";
```

`inline-signing` **enables** `ixfr-from-differences`

Slave Model

* In the slave model, a BIND 9.9 server transfers the unsigned zone data from an existing DNS server.
* This server does not need to be BIND.
* We'd like it to be of course...

Slave Model Configuration

Without Inline-Signing

```
zone "example.net" {
  type slave;
  masters { 1.2.3.4; };
  file "slave/example.net";
};
```

Slave Model Configuration

With Inline-Signing

```
zone "example.net" {
  type slave;
  masters { 1.2.3.4; };
  file "slave/example.net";
  inline-signing yes;
  auto-dnssec maintain;
  key-directory "keys";
};
```

File Model

- In the file model, a BIND 9.9 server loads the unsigned zone data from a file on your disk.
- This allows manually editing your zone files, just like you may do today.
- This allows existing scripts to generate zone data.

File Model Configuration

Without Inline-Signing

```
zone "example.net" {
  type master;
  file "master/example.net";
};
```

File Model Configuration

With Inline-Signing

```
zone "example.net" {
  type master;
  file "master/example.net";
  inline-signing yes;
  auto-dnssec maintain;
  key-directory "keys";
};
```

Key Generation

```
$ cd /var/named

$ dnssec-keygen -K ./keys -f KSK example.net

$ dnssec-keygen -K ./keys example.net
```

* Check the `directory` statement in the `options` block.
* Set other key parameters as needed (length, key type, etc)

Key Management

- Key management is large topic.

- Key generation and storage:
  - Use an HSM if you need to
  - Perhaps use an HSM for KSK, files for ZSK
  - Select appropriately sized keys

- General key rolling guidelines:
  - Roll enough to know how, but not more often
  - Roll when there is a reason to.

Any questions?

Wow, that was a lot to digest!

Check http://kb.isc.org for inline-signing, DNSSEC, and many other topics

We'll have an inline-signing article up soon!

Reducing Risk

DNSSEC is new.

Many people do not have solid operational experience.

DNSSEC is scary.

Once your parent zone has your KSK, there's no going back without causing failures.

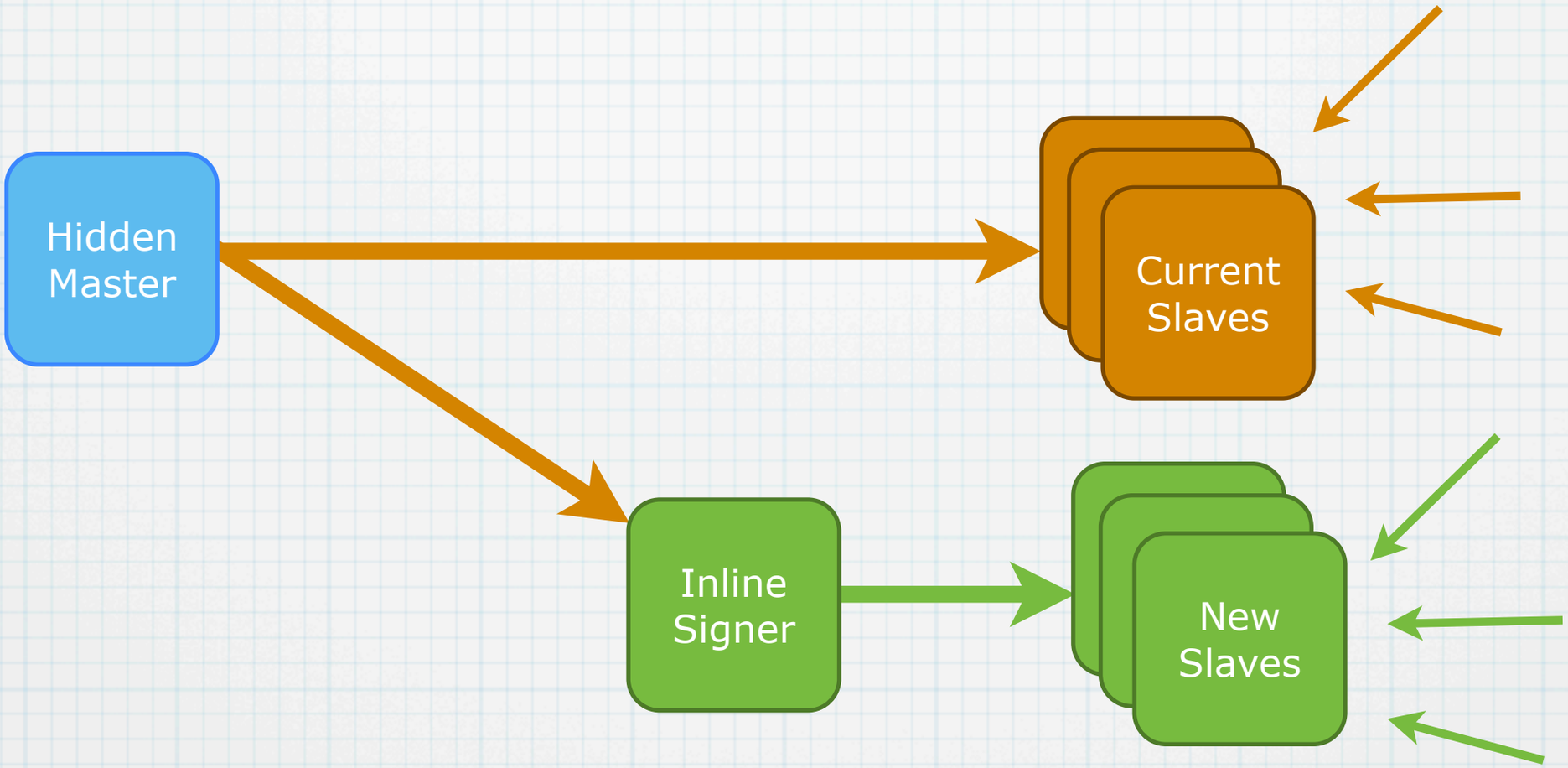
We suggest finding a safe approach.

Each situation is unique. ISC is here to help.

Parallel Deployment

- Reduces risk by reducing changes
  - Existing infrastructure is mostly untouched
- Add servers to handle the signed data
  - You might want to upgrade them anyway
- Easy to switch back to unsigned
  - Maybe
- Allows testbed or selective exposure

Parallel Deployment



Gimme!

- Early February for final release
- Get the Release Candidate #1 *today*
- Sign up for the `bind-announce` list to receive release notifications

  https://lists.isc.org/mailman/listinfo/bind-announce

Upcoming Training

- 2-Day Introductory DNS & BIND Training, Feb 6-7, Singapore
- 5-Day Intro & Advanced DNS & BIND Topics (incl. DNSSEC), Feb 6-10, Singapore
- 3-Day IPv6 Fundamentals Workshop, Feb 13-15, Melbourne, Australia
- 2-Day ISC DHCP Workshop, Feb 16-17, Melbourne, Australia
- 3-Day DNSSEC Implementation and Deployment Workshop, Feb-Mar TBD, West Coast, USA
- 2-Day Introductory DNS & BIND Training, Mar 12-13, Rome, Italy
- 5-Day Intro & Advanced DNS & BIND Topics (incl. DNSSEC), Mar 12-16, Rome, Italy
- 3-Day IPv6 Fundamentals Workshop, Mar 19-21, Berlin, Germany
- 2-Day ISC DHCP Workshop, Mar 22-23, Berlin, Germany
- 3-Day DNSSEC Implementation and Deployment Workshop, May 15-17, Basingstoke, UK
- 5-Day Intro & Advanced DNS & BIND Topics (incl. DNSSEC) June TBD, East Coast, USA
- 3-Day IPv6 Fundamentals Workshop, June 4-6, Amsterdam, NL
- 2-Day ISC DHCP Workshop, June 7-8, Amsterdam, NL
- 2-Day Introductory DNS & BIND Training, June 11-12, Amsterdam, NL
- 5-Day Intro & Advanced DNS & BIND Topics (incl. DNSSEC), June 11-15, Amsterdam, NL

Upcoming Web Seminars

Next Web Seminar: January 25, 2012

ISC Product Updates: BIND, DHCP, PCP, and more... what's going to be hot at ISC in 2012

Please note that this webinar is offered as a benefit to ISC Members, Customers and Forum Sponsors only. If you would like to receive this benefit, please email sales@isc.org

Coming Soon:

Secondary Name Server (SNS) - 8 February 2012

Secondary Name Server (SNS) 8 Feb 2012 - in Spanish - 22 Feb 2012

Cyber-Crime - Passive DNS & DNSRPZ - 7 Mar 2012

Coming Soon!

DNS Resiliency; Why is it so critical

Training Certification

Registry Services

Ops Chat: Anycast

Sign up for upcoming sessions or view previous session archives at

http://www.isc.org/webinars

Special Offer for Attendees

Choose one:

20% Off

5-day BIND with DNSSEC training

20% Off

3-day DNSSEC training workshop

20% Off

BIND Configuration Review for DNSSEC Readiness consulting

Training offers are valid for training sessions offered by ISC through June 30, 2012. You must sign up within 30 days of attending this presentation to receive this discount.

Consulting is provided through ISC's consulting services. For more information, please see https://www.isc.org/support/consulting or contact your account manager for details.

Keeping in Contact

http://www.facebook.com/InternetSystemsConsortium

http://www.linkedin.com/company/internet-systems-consortium

http://twitter.com/ISCdotORG

ISC Resources

Knowledge Base for many things

http://kb.isc.org/

bind-announce for release notifications

http://lists.isc.org/mailman/listinfo/bind-announce

bind-users for community assistance

http://lists.isc.org/mailman/listinfo/bind-users

Questions?

Thank you for attending.

www.isc.org