BIND 9.9 Feature Overview

November 30, 2011

Copyright (c) 2011 Internet Systems Consortium

About the Presenters

Michael Graff

BIND 9 Engineering Manager

mgraff@isc.org

@skandragon

Larissa Shapiro

ISC Product Manager

larissas@isc.org

@larissashapiro

Copyright (c) 2011 Internet Systems Consortium

Agenda

- Introductions & Logistics
- ISC Overview
- BIND 9.9 Feature Preview
- ISC Services and DNSSEC
- Questions

Copyright (c) 2011 Internet Systems Consortium

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

Copyright (c) 2011 Internet Systems Consortium

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)

Copyright (c) 2011 Internet Systems Consortium

What's Coming in BIND 9.9?

Copyright (c) 2011 Internet Systems Consortium

What's Coming in BIND 9.9?

- New and changed `rndc` commands

Copyright (c) 2011 Internet Systems Consortium

What's Coming in BIND 9.9?

- New and changed `rndc` commands
- Performance

Copyright (c) 2011 Internet Systems Consortium

What's Coming in BIND 9.9?

- New and changed `rndc` commands
- Performance
- Minor features and changes

Copyright (c) 2011 Internet Systems Consortium

What's Coming in BIND 9.9?

- New and changed `rndc` commands
- Performance
- Minor features and changes
- Major features

Copyright (c) 2011 Internet Systems Consortium

New and Changed `rndc` Commands

Copyright (c) 2011 Internet Systems Consortium

New and Changed `rndc` Commands

- `flushtree` deletes tree from cache
  - `rndc flushtree example.com`

Copyright (c) 2011 Internet Systems Consortium

New and Changed `rndc` Commands

- `flushtree` deletes tree from cache
  - `rndc flushtree example.com`

- `sync` to write zone to file
  - "`sync -clean`" removes journal as well

Copyright (c) 2011 Internet Systems Consortium

New and Changed `rndc` Commands

- `flushtree` deletes tree from cache
  - `rndc flushtree example.com`

- `sync` to write zone to file
  - "`sync -clean`" removes journal as well

- `freeze` / `thaw` do not remove journal
  - `-ixfr-from-differences` + dynamic zones

Copyright (c) 2011 Internet Systems Consortium

New and Changed `rndc` Commands

- `flushtree` deletes tree from cache
  - `rndc flushtree example.com`
- `sync` to write zone to file
  - "`sync -clean`" removes journal as well
- `freeze` / `thaw` do not remove journal
  - `-ixfr-from-differences` + dynamic zones
- `reconfig` performance

Copyright (c) 2011 Internet Systems Consortium

Performance: Zone Loading

Copyright (c) 2011 Internet Systems Consortium

Performance: Zone Loading

- Many small zones
  - 100k to 1m, 20 to 100 records each

Copyright (c) 2011 Internet Systems Consortium

Performance: Zone Loading

- Many small zones
  - 100k to 1m, 20 to 100 records each
- Also improves shutdown

Copyright (c) 2011 Internet Systems Consortium

Performance: Zone Loading

- Many small zones
  - 100k to 1m, 20 to 100 records each
- Also improves shutdown
- Slight memory increase
  - About 2.3% at 500k zones

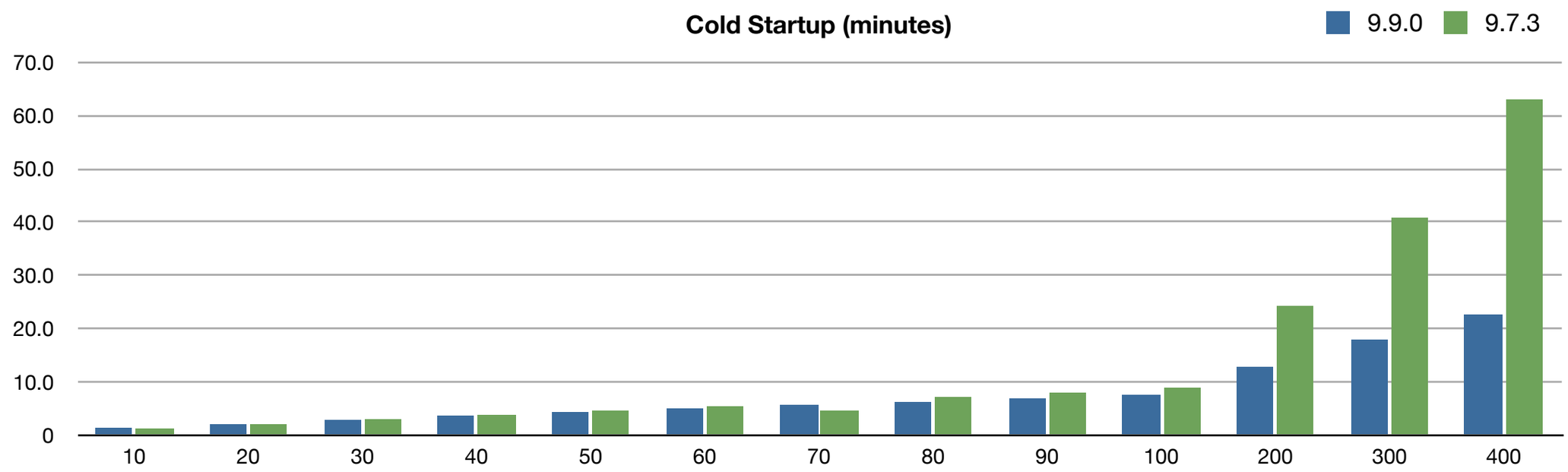
Copyright (c) 2011 Internet Systems Consortium

Performance: Zone Loading

- Many small zones
  - 100k to 1m, 20 to 100 records each
- Also improves shutdown
- Slight memory increase
  - About 2.3% at 500k zones
- Customer reported speedups: 3x - 20x

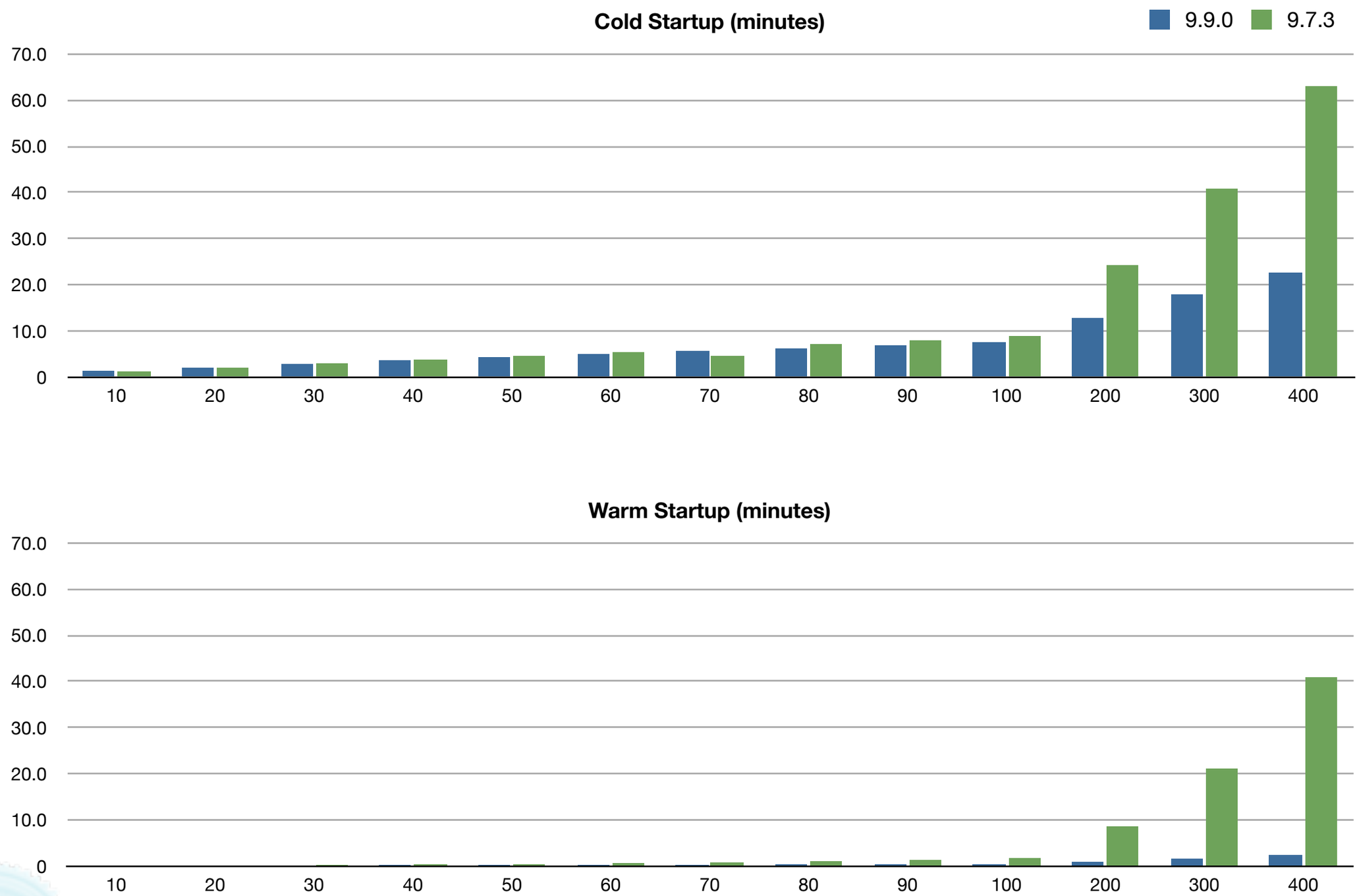
Copyright (c) 2011 Internet Systems Consortium

Performance: Zone Loading



Copyright (c) 2011 Internet Systems Consortium

Performance: Zone Loading



Copyright (c) 2011 Internet Systems Consortium

Performance: Multicore

Copyright (c) 2011 Internet Systems Consortium

Performance: Multicore

- Authoritative and recursive

Copyright (c) 2011 Internet Systems Consortium

Performance: Multicore

- Authoritative and recursive
- Spreads network I/O across threads
  - Only benefits threaded builds (`named -V`)

Copyright (c) 2011 Internet Systems Consortium

Performance: Multicore

- Authoritative and recursive

- Spreads network I/O across threads
  - Only benefits threaded builds (`named -V`)

- High QPS environments

Copyright (c) 2011 Internet Systems Consortium

Performance: Multicore

- Authoritative and recursive
- Spreads network I/O across threads
  - Only benefits threaded builds (`named -V`)
- High QPS environments
- 6 or more cores

Copyright (c) 2011 Internet Systems Consortium

Performance

Copyright (c) 2011 Internet Systems Consortium

Minor Features

Copyright (c) 2011 Internet Systems Consortium

Minor Features

- Statistics from `dnssec-signzone`

Copyright (c) 2011 Internet Systems Consortium

Minor Features

- Statistics from `dnssec-signzone`
- Set TTL for keys during generation

Copyright (c) 2011 Internet Systems Consortium

Minor Features

- Statistics from `dnssec-signzone`
- Set TTL for keys during generation
- Combined signing key “CSK”

Copyright (c) 2011 Internet Systems Consortium

Minor Features

- Statistics from `dnssec-signzone`
- Set TTL for keys during generation
- Combined signing key “CSK”
- Start with NSEC3

Copyright (c) 2011 Internet Systems Consortium

Minor Features

Copyright (c) 2011 Internet Systems Consortium

Minor Features

- Different expiration for DNSKEYs

Copyright (c) 2011 Internet Systems Consortium

Minor Features

- Different expiration for DNSKEYs
- Human-readable DNSKEYs from `dig`

Copyright (c) 2011 Internet Systems Consortium

Minor Features

- Different expiration for DNSKEYs
- Human-readable DNSKEYs from `dig`
- `also-notify` syntax matches `masters`

Copyright (c) 2011 Internet Systems Consortium

Minor Features

- Different expiration for DNSKEYs
- Human-readable DNSKEYs from `dig`
- `also-notify` syntax matches `masters`
- `serial-update-method` option

Copyright (c) 2011 Internet Systems Consortium

Minor Features

Copyright (c) 2011 Internet Systems Consortium

Major Features

Copyright (c) 2011 Internet Systems Consortium

Major Features

NXDOMAIN Redirection

Copyright (c) 2011 Internet Systems Consortium

Major Features

NXDOMAIN Redirection

Stand-aside signing

Copyright (c) 2011 Internet Systems Consortium

Major Features

NXDOMAIN Redirection

Stand-aside signing

Inline signing

Copyright (c) 2011 Internet Systems Consortium

NXDOMAIN Redirection

Copyright (c) 2011 Internet Systems Consortium

NXDOMAIN Redirection

- Controversial

Copyright (c) 2011 Internet Systems Consortium

NXDOMAIN Redirection

- Controversial
- Disabled for DNSSEC clients

Copyright (c) 2011 Internet Systems Consortium

NXDOMAIN Redirection

- Controversial
- Disabled for DNSSEC clients
- Allows rewriting negative answers

Copyright (c) 2011 Internet Systems Consortium

NXDOMAIN Redirection

- Controversial
- Disabled for DNSSEC clients
- Allows rewriting negative answers
- Destination specified in special zone

Copyright (c) 2011 Internet Systems Consortium

NXDOMAIN Redirection

Copyright (c) 2011 Internet Systems Consortium

Stand-Aside Signing

Copyright (c) 2011 Internet Systems Consortium

Stand-Aside Signing

- IPAM or other non-DDnS data source

Copyright (c) 2011 Internet Systems Consortium

Stand-Aside Signing

- IPAM or other non-DDnS data source
- Want to sign zone data

Copyright (c) 2011 Internet Systems Consortium

Stand-Aside Signing

- IPAM or other non-DDnS data source
- Want to sign zone data
- Have large or many zones

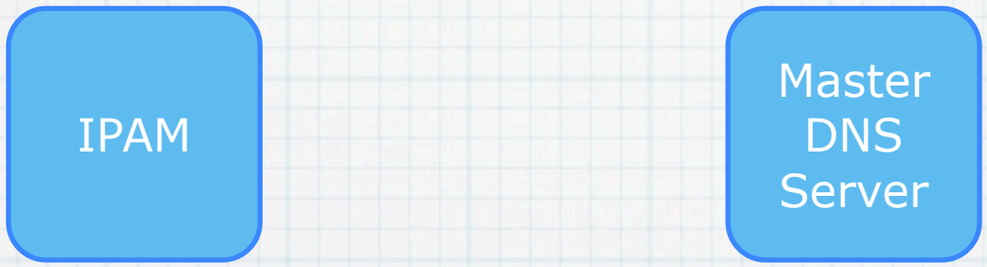
Copyright (c) 2011 Internet Systems Consortium

Stand-Aside Signing

- IPAM or other non-DDnS data source
- Want to sign zone data
- Have large or many zones
- Reduces IXFR-style transfer size

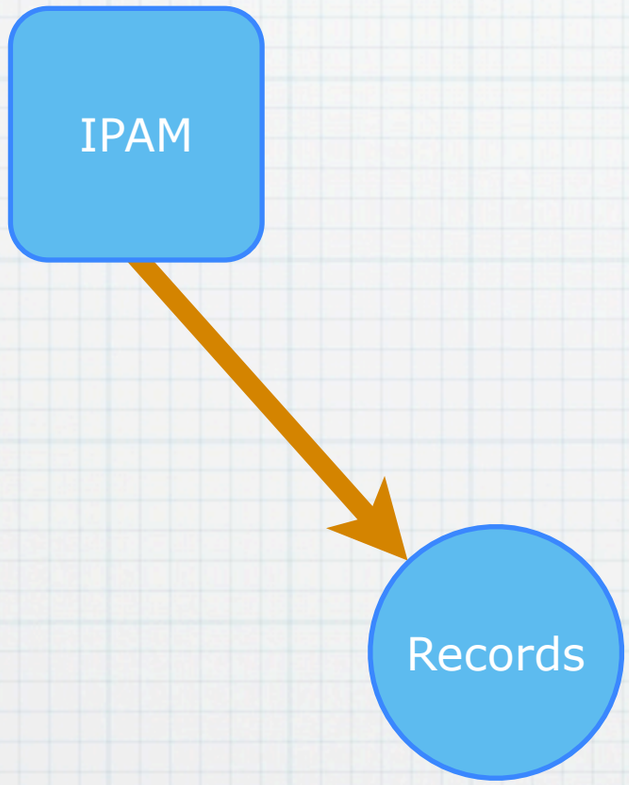
Copyright (c) 2011 Internet Systems Consortium

Before DNSSEC



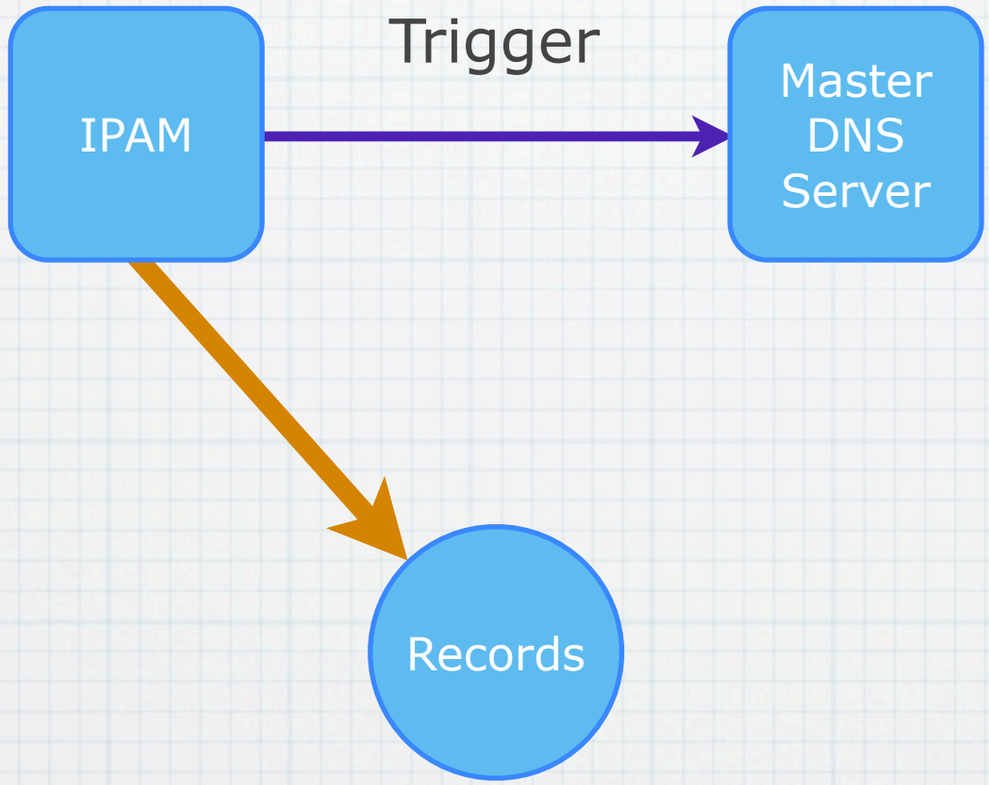
Copyright (c) 2011 Internet Systems Consortium

Before DNSSEC



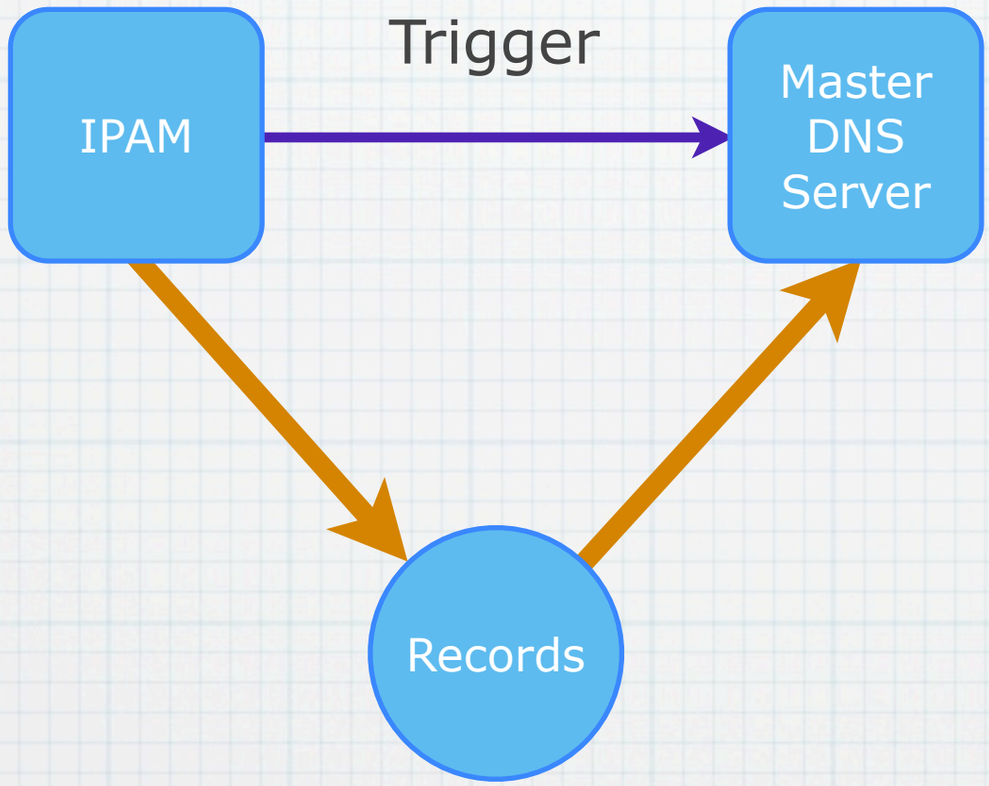
Copyright (c) 2011 Internet Systems Consortium

Before DNSSEC



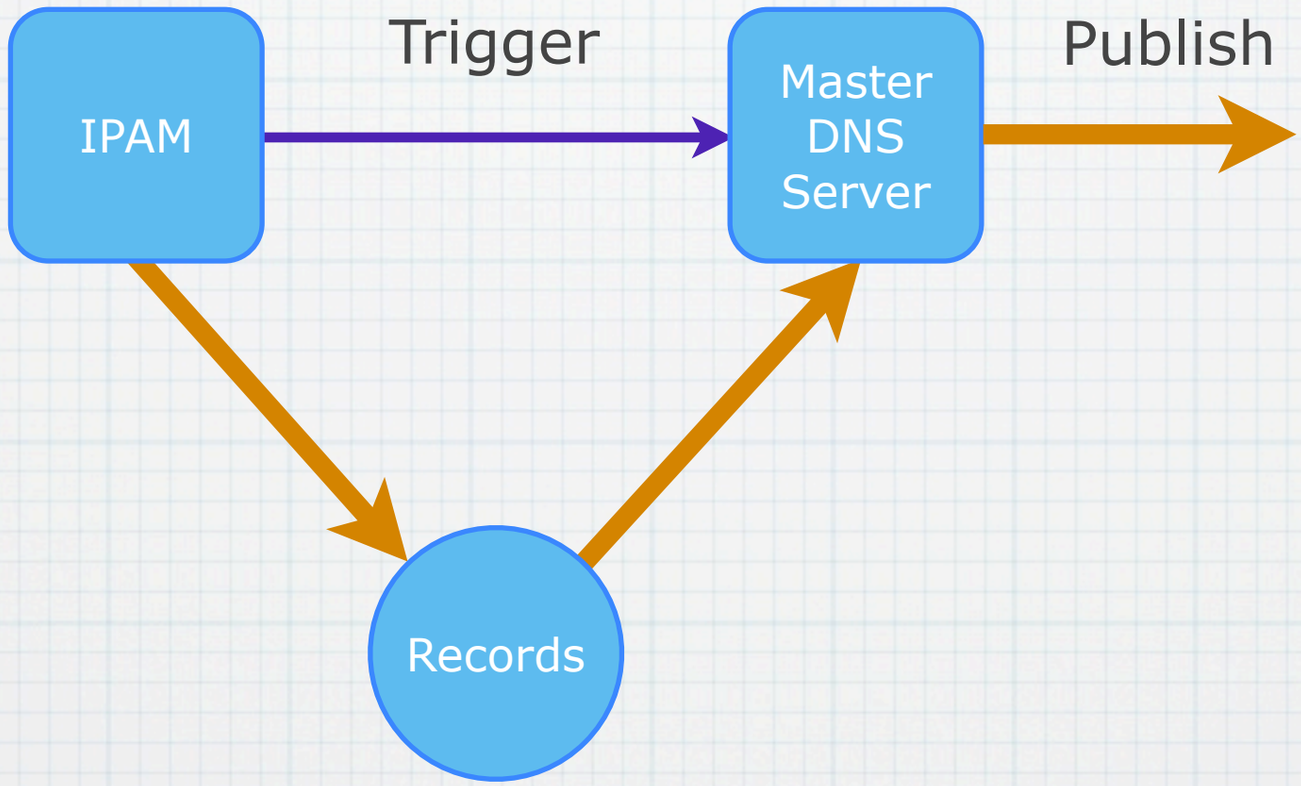
Copyright (c) 2011 Internet Systems Consortium

Before DNSSEC



Copyright (c) 2011 Internet Systems Consortium

Before DNSSEC

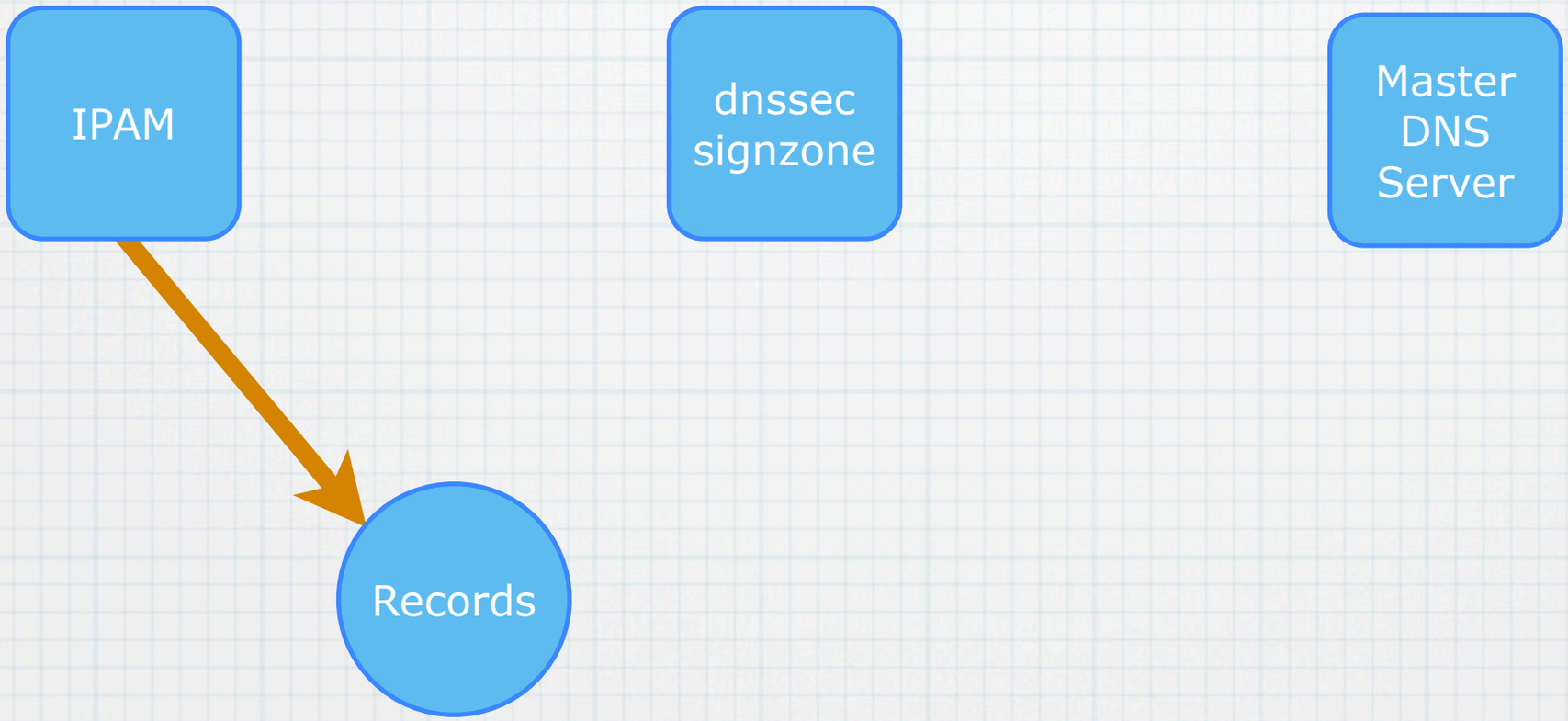


Copyright (c) 2011 Internet Systems Consortium

Before Stand-Aside

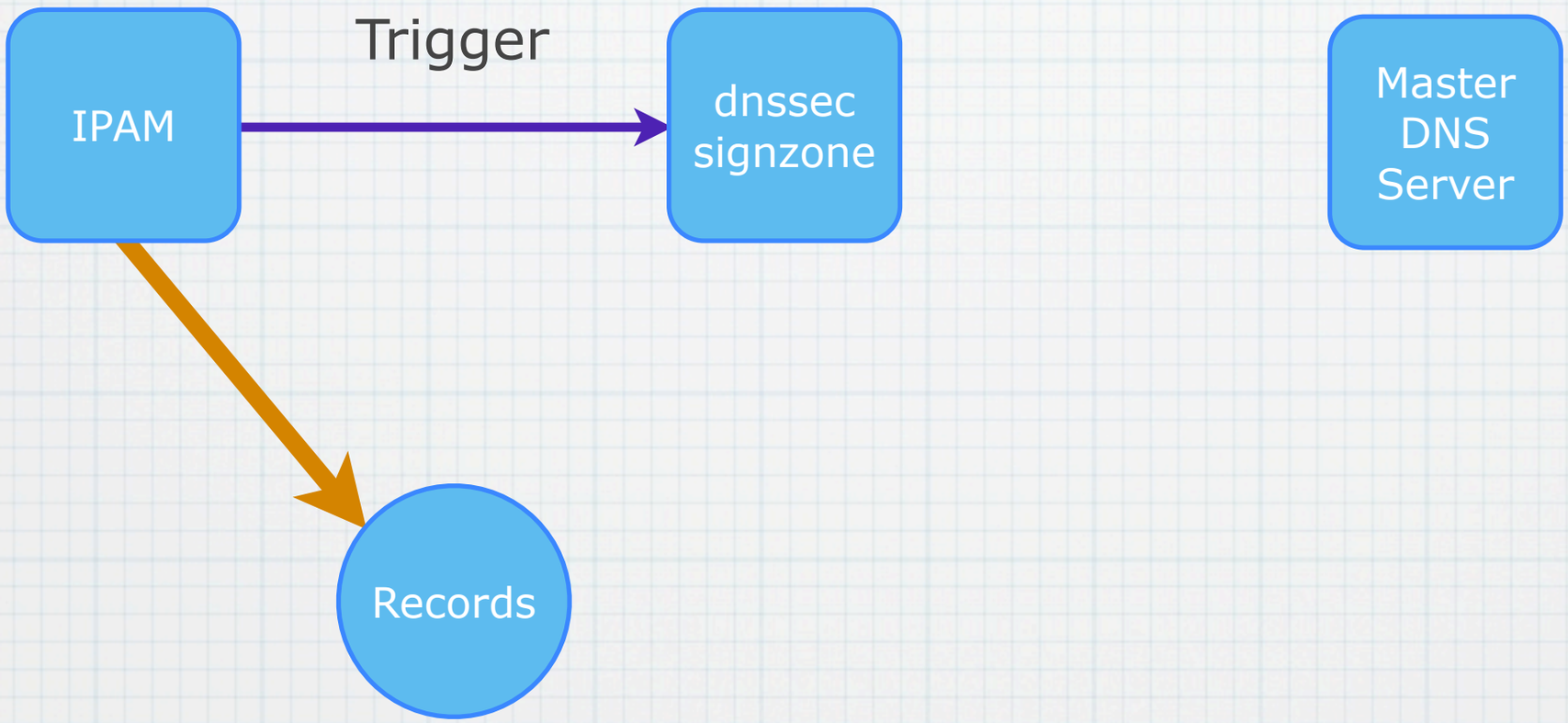
Copyright (c) 2011 Internet Systems Consortium

Before Stand-Aside



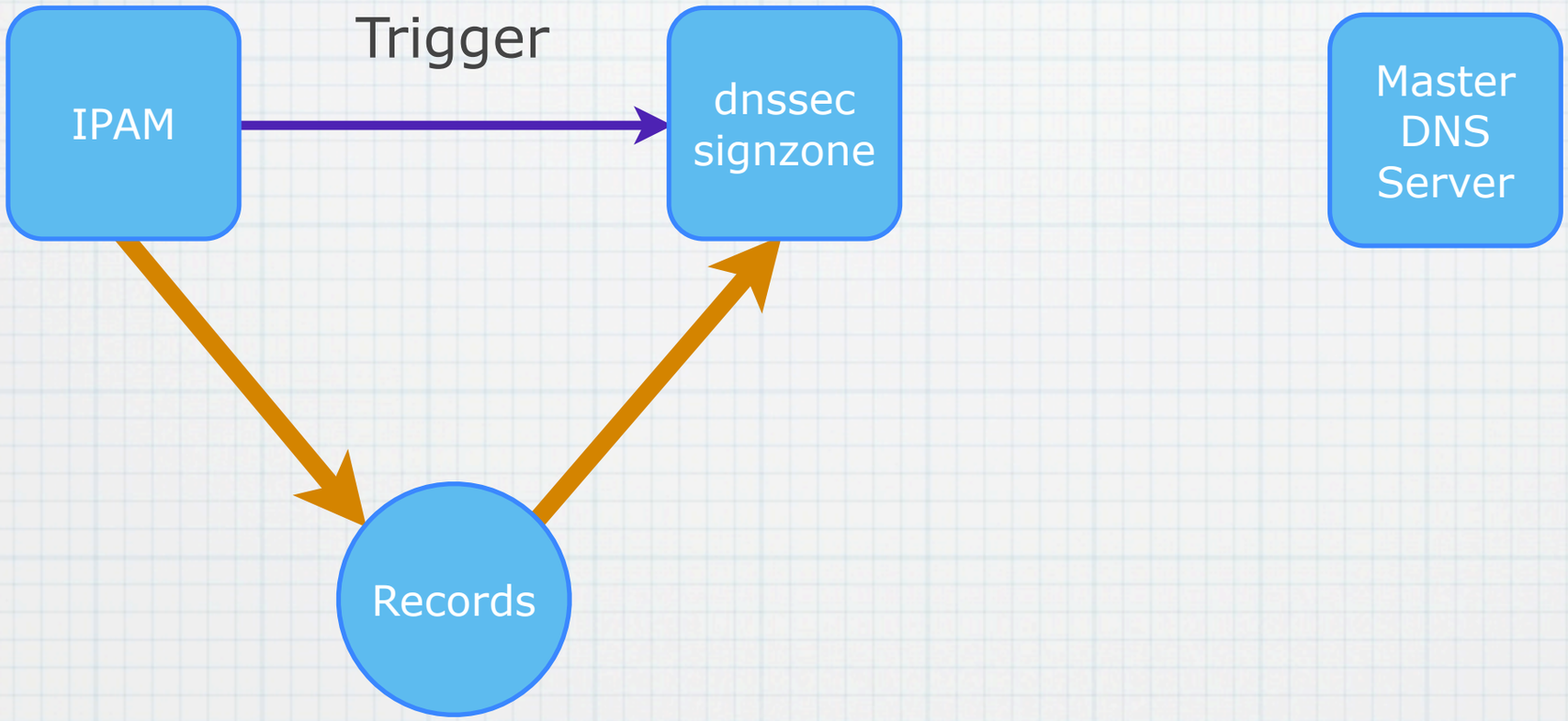
Copyright (c) 2011 Internet Systems Consortium

Before Stand-Aside



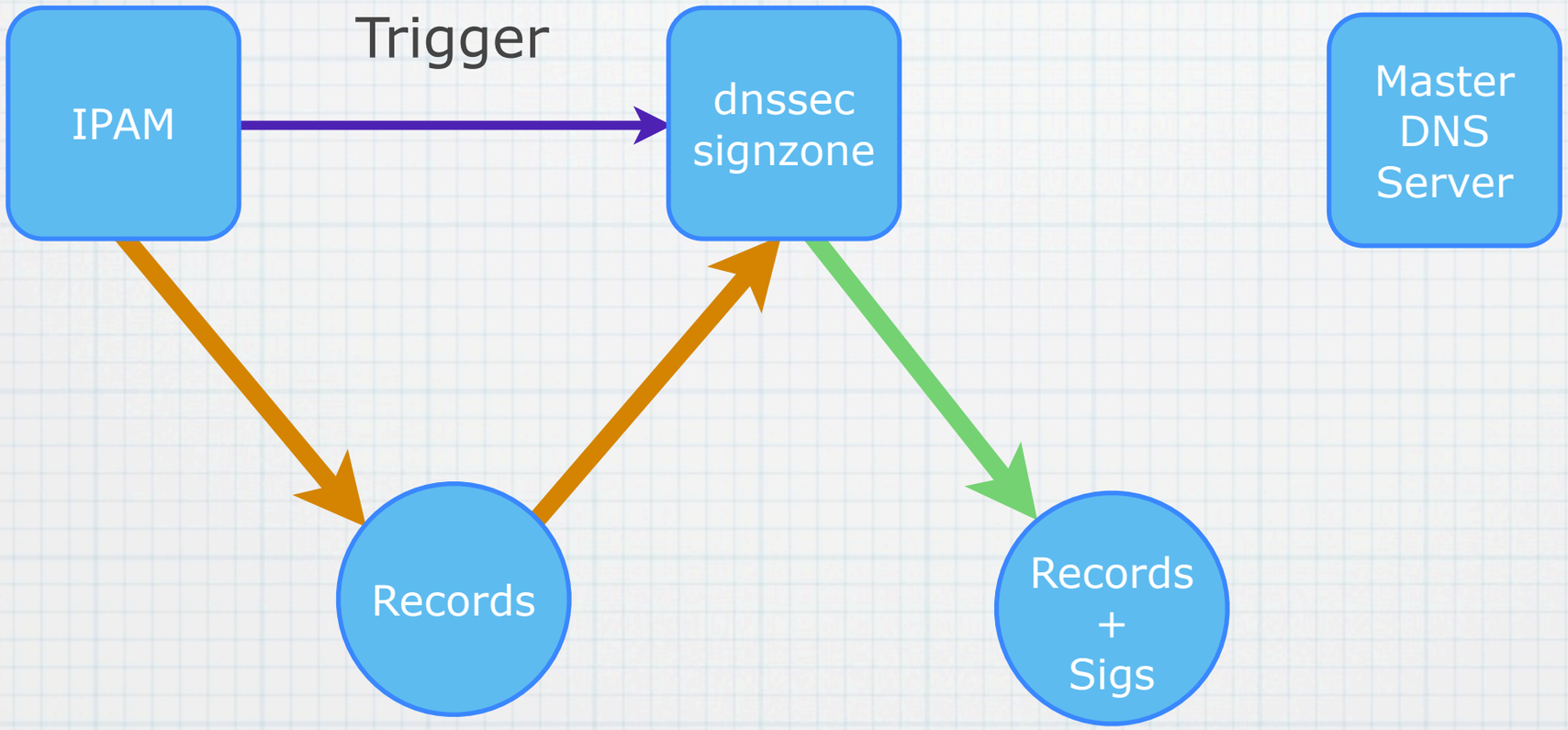
Copyright (c) 2011 Internet Systems Consortium

Before Stand-Aside



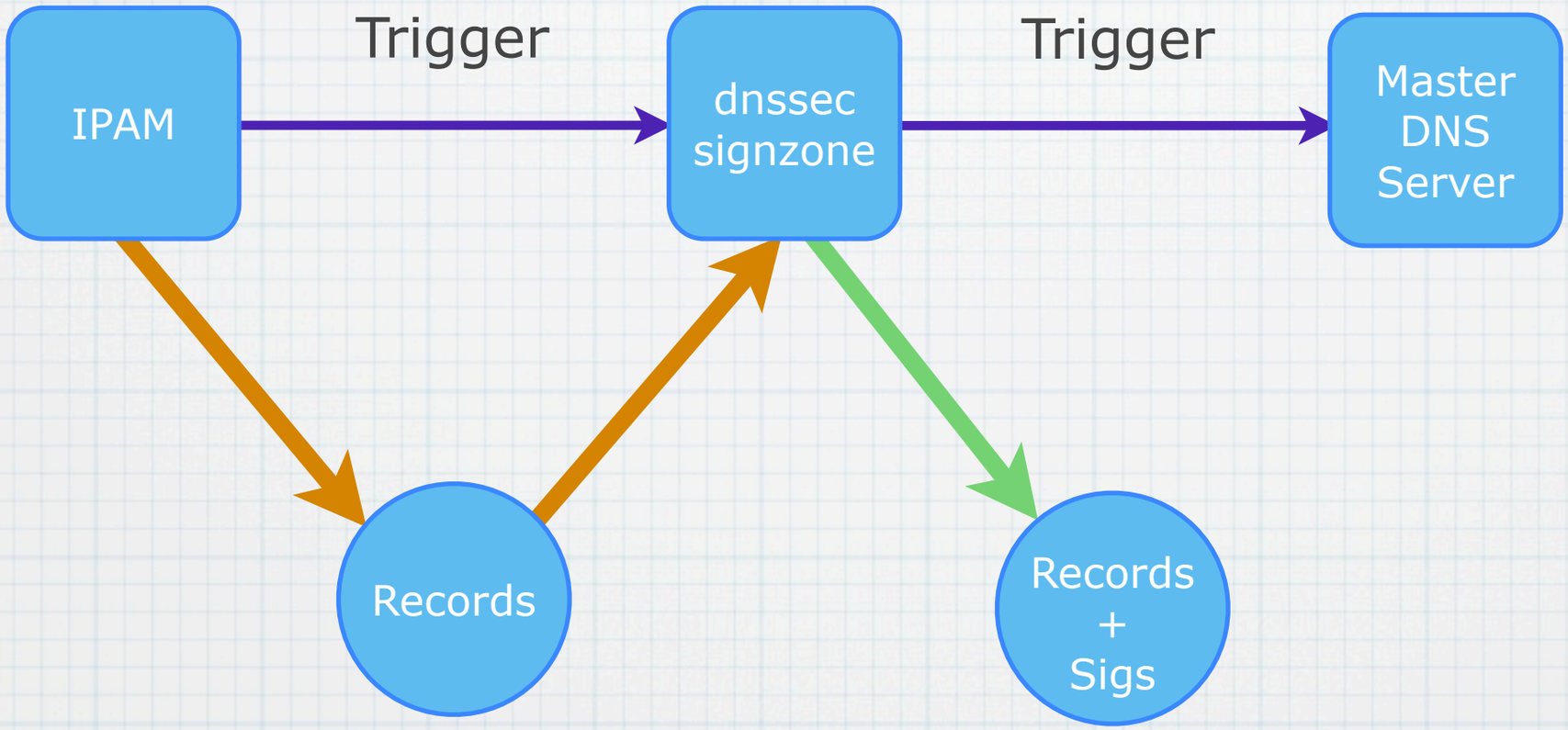
Copyright (c) 2011 Internet Systems Consortium

Before Stand-Aside



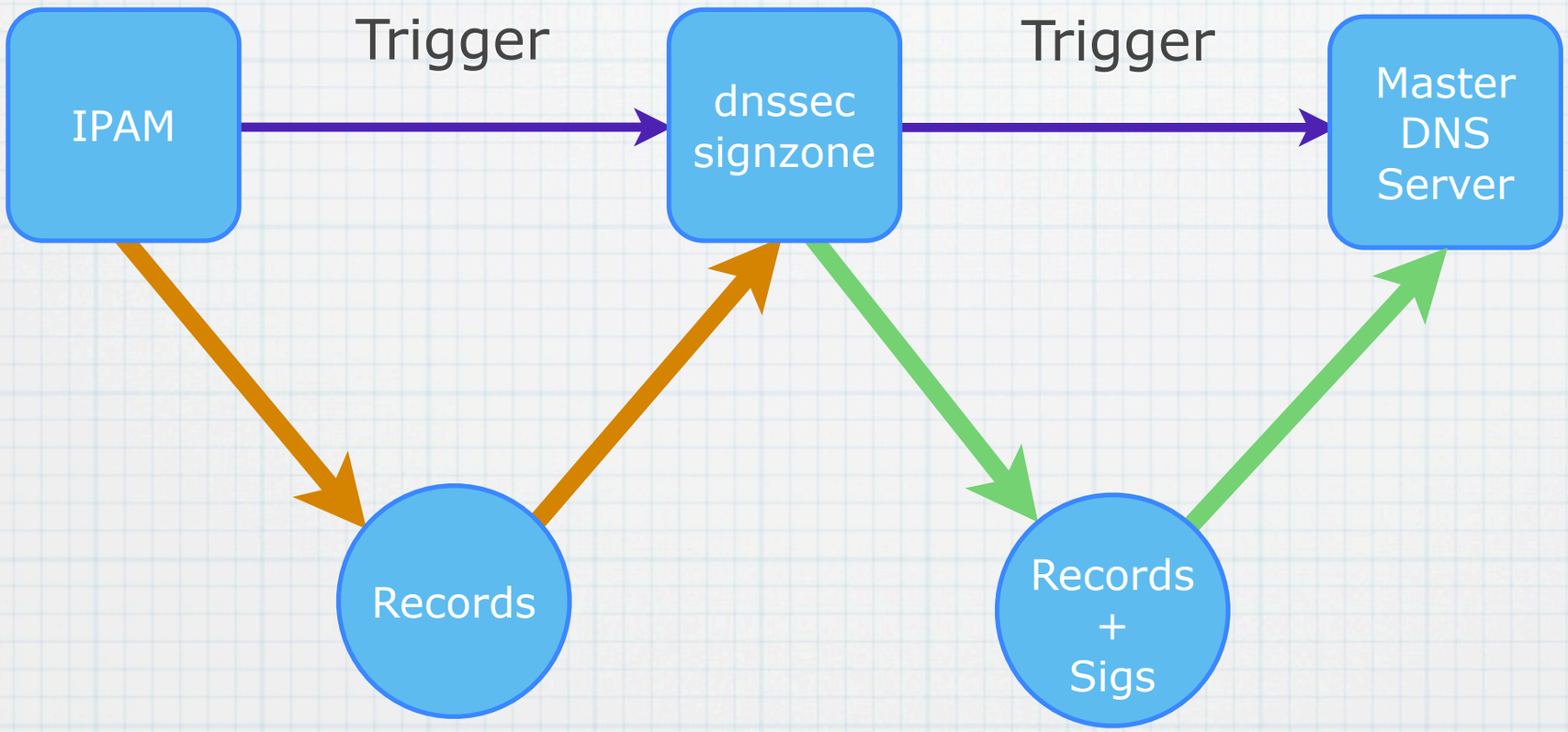
Copyright (c) 2011 Internet Systems Consortium

Before Stand-Aside



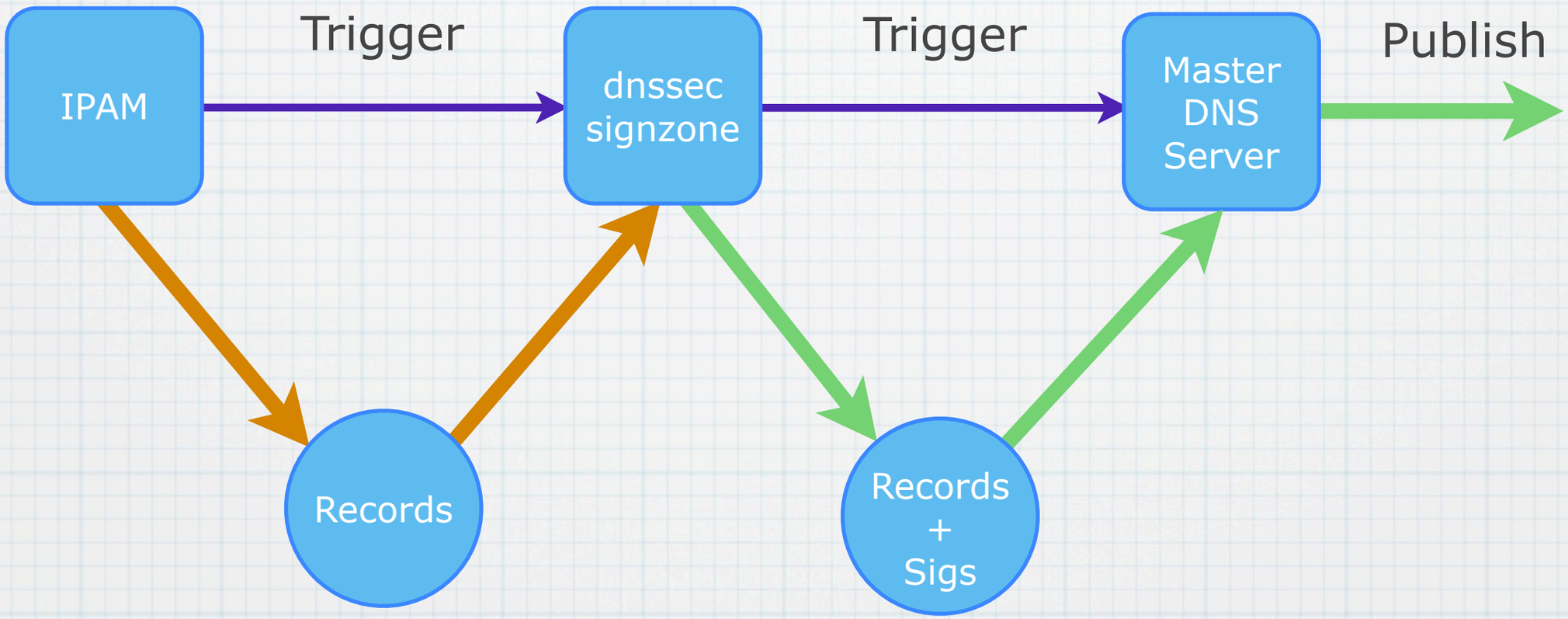
Copyright (c) 2011 Internet Systems Consortium

Before Stand-Aside



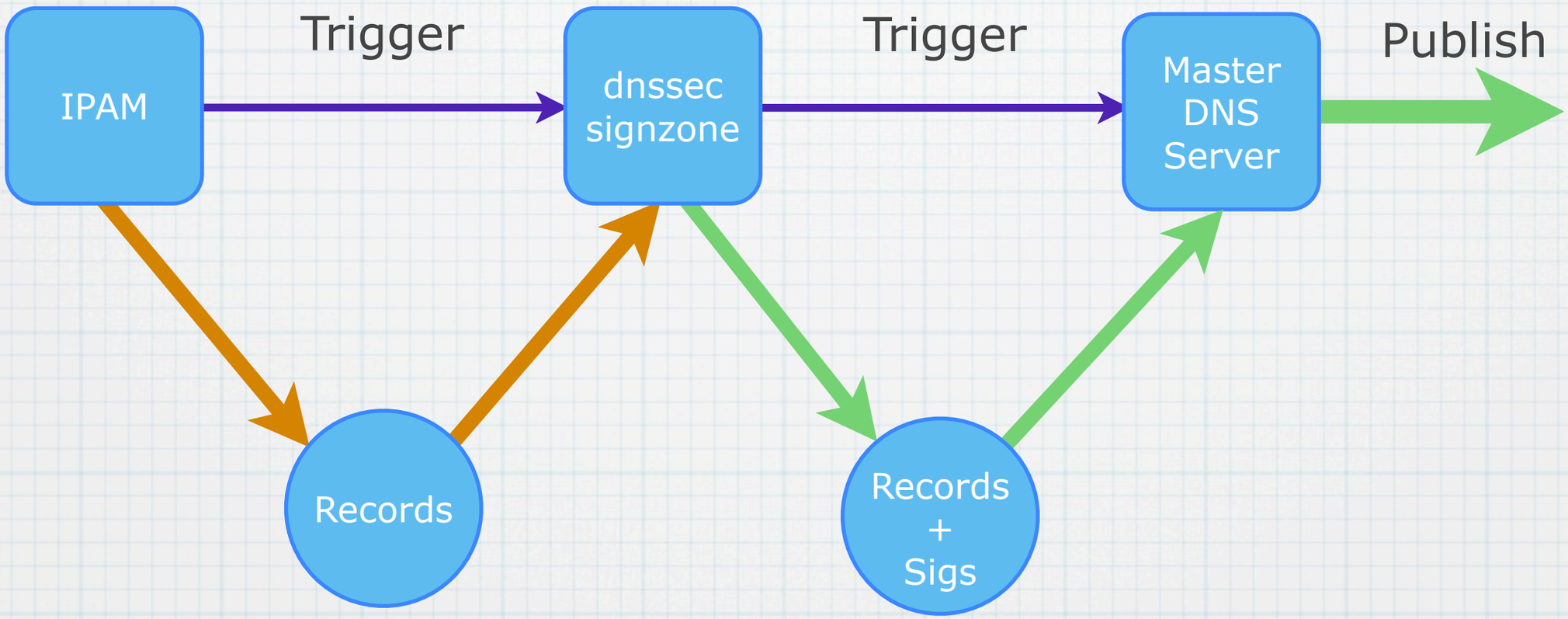
Copyright (c) 2011 Internet Systems Consortium

Before Stand-Aside



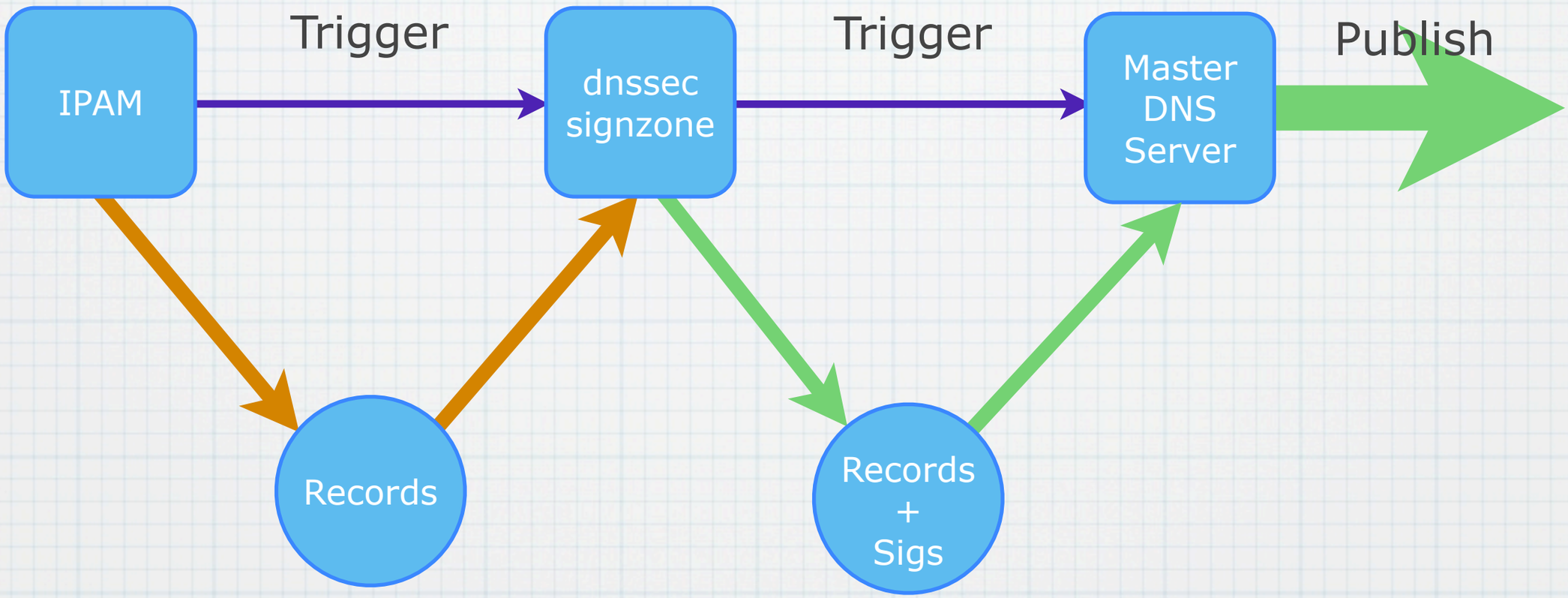
Copyright (c) 2011 Internet Systems Consortium

Before Stand-Aside



Copyright (c) 2011 Internet Systems Consortium

Before Stand-Aside

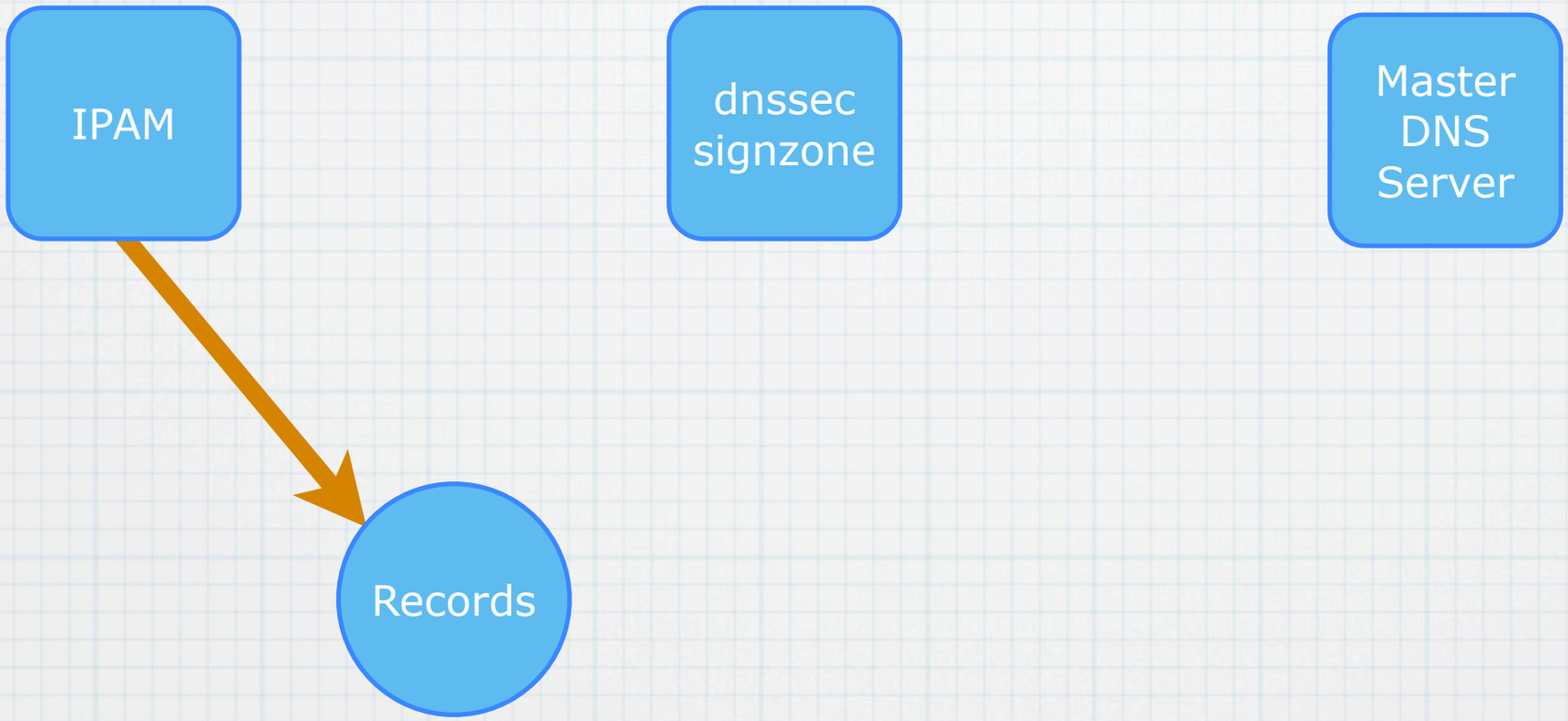


Copyright (c) 2011 Internet Systems Consortium

First Signing

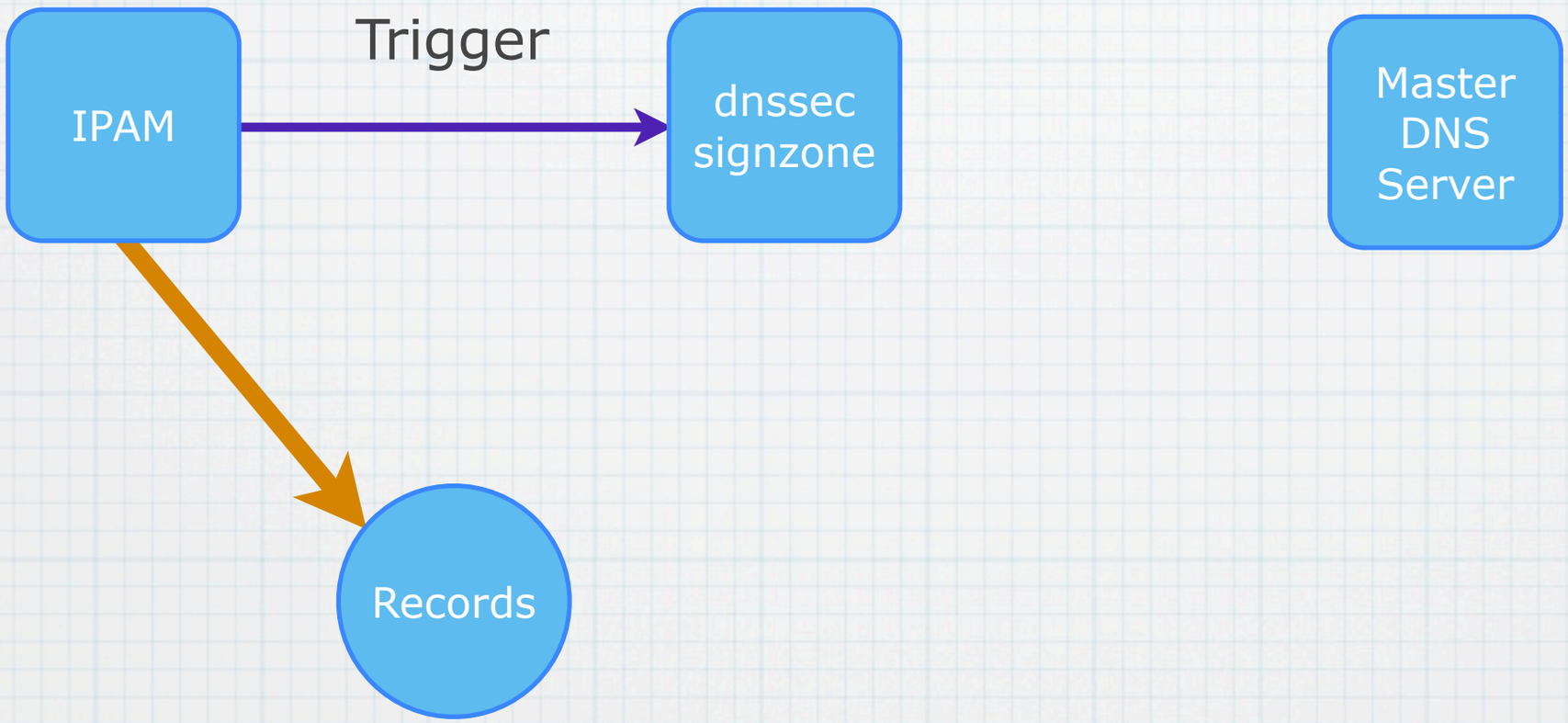
Copyright (c) 2011 Internet Systems Consortium

First Signing



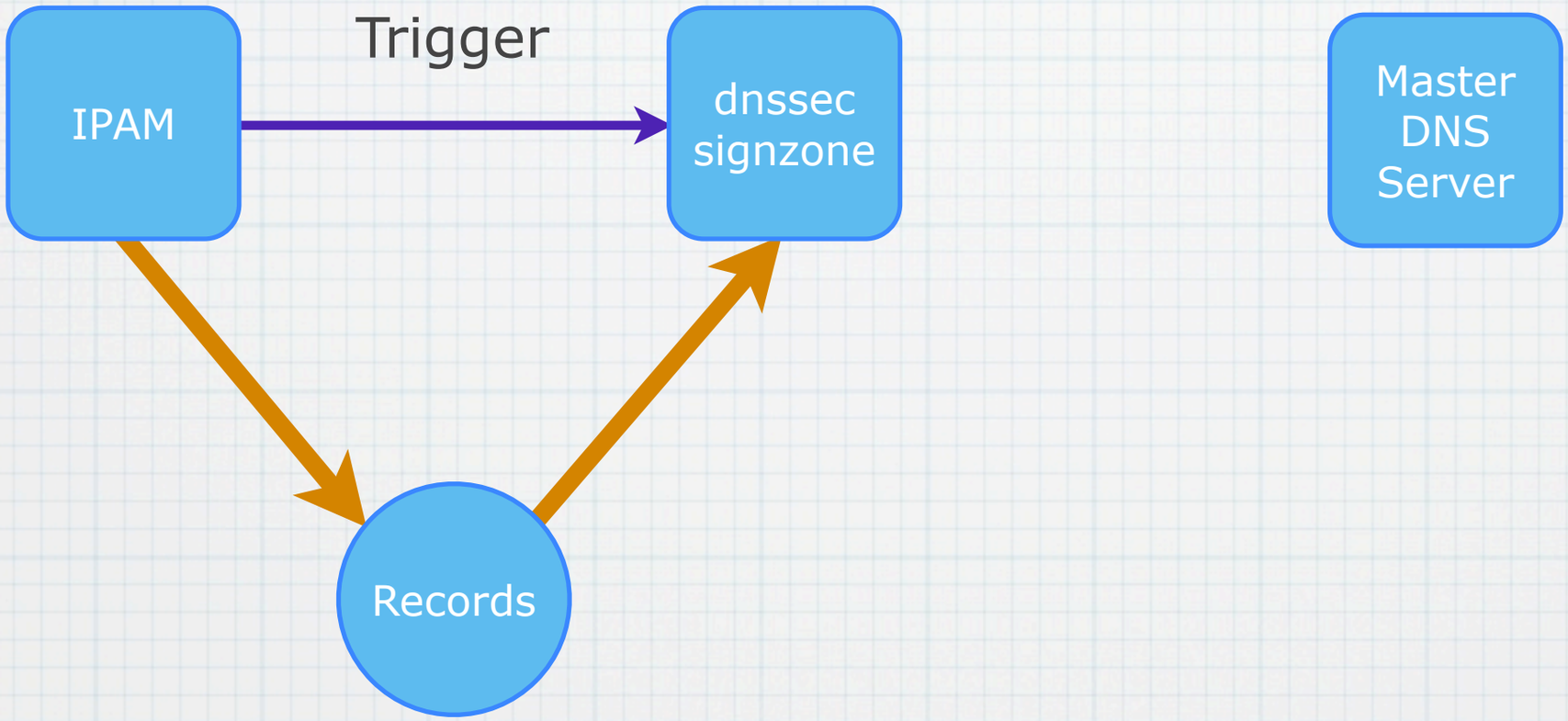
Copyright (c) 2011 Internet Systems Consortium

First Signing



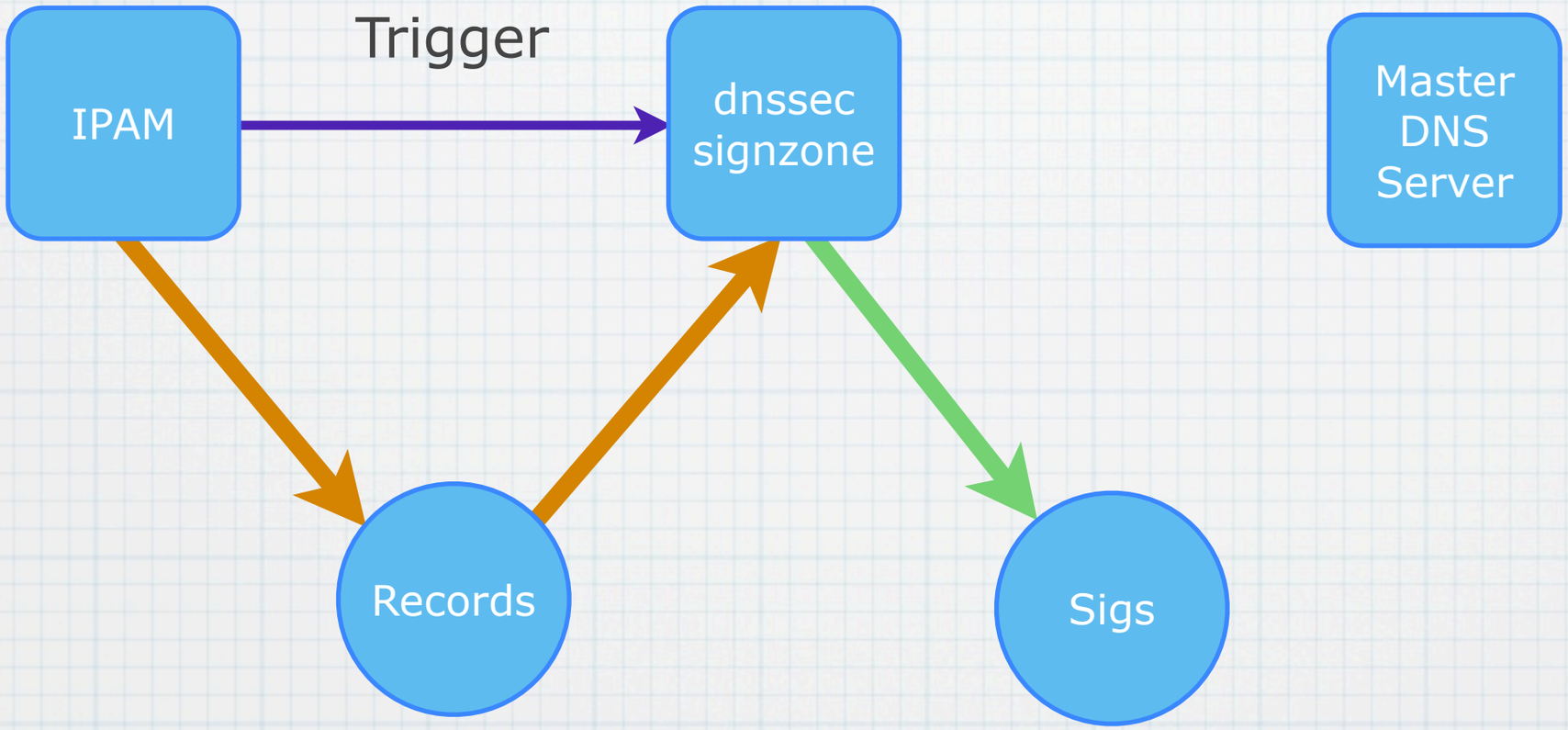
Copyright (c) 2011 Internet Systems Consortium

First Signing



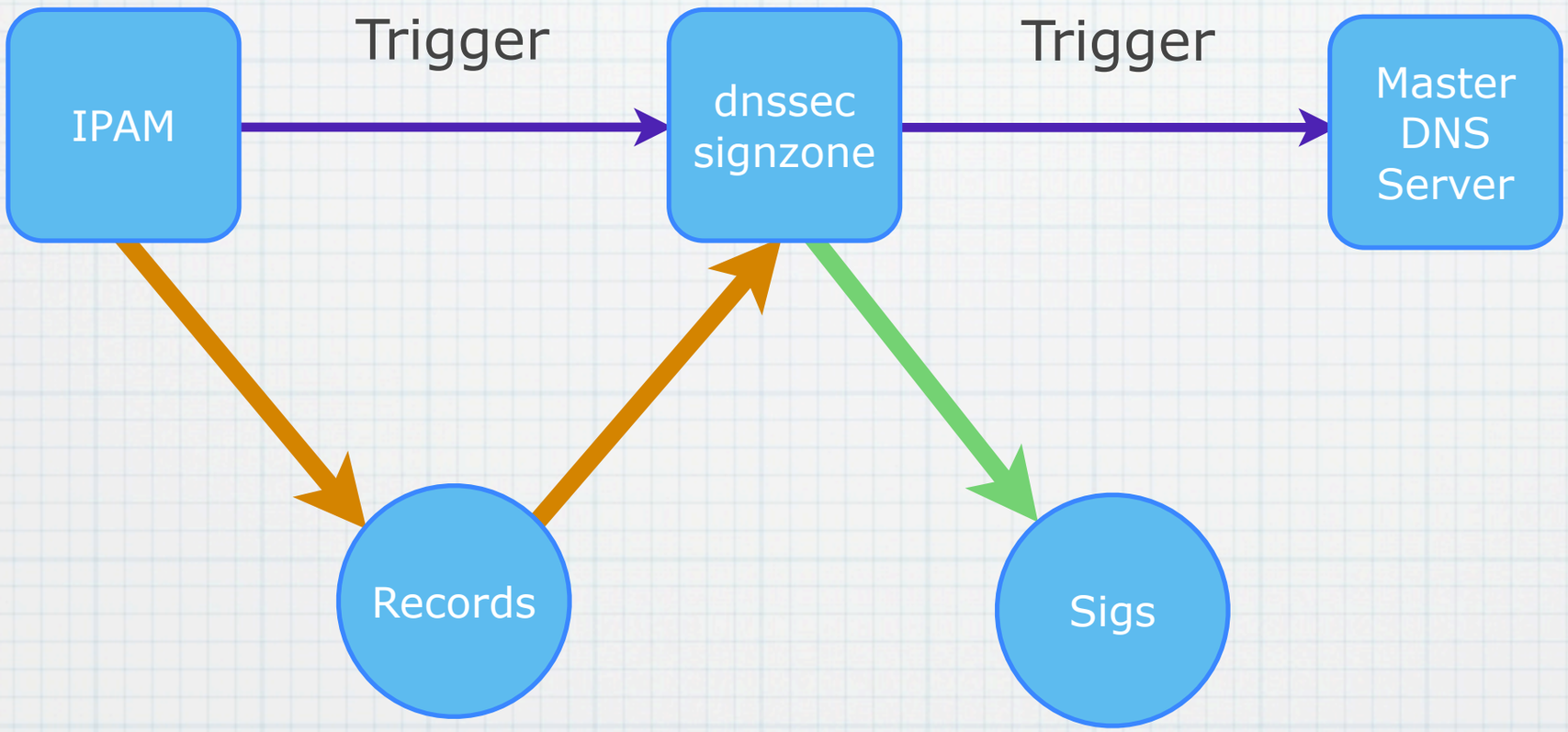
Copyright (c) 2011 Internet Systems Consortium

First Signing



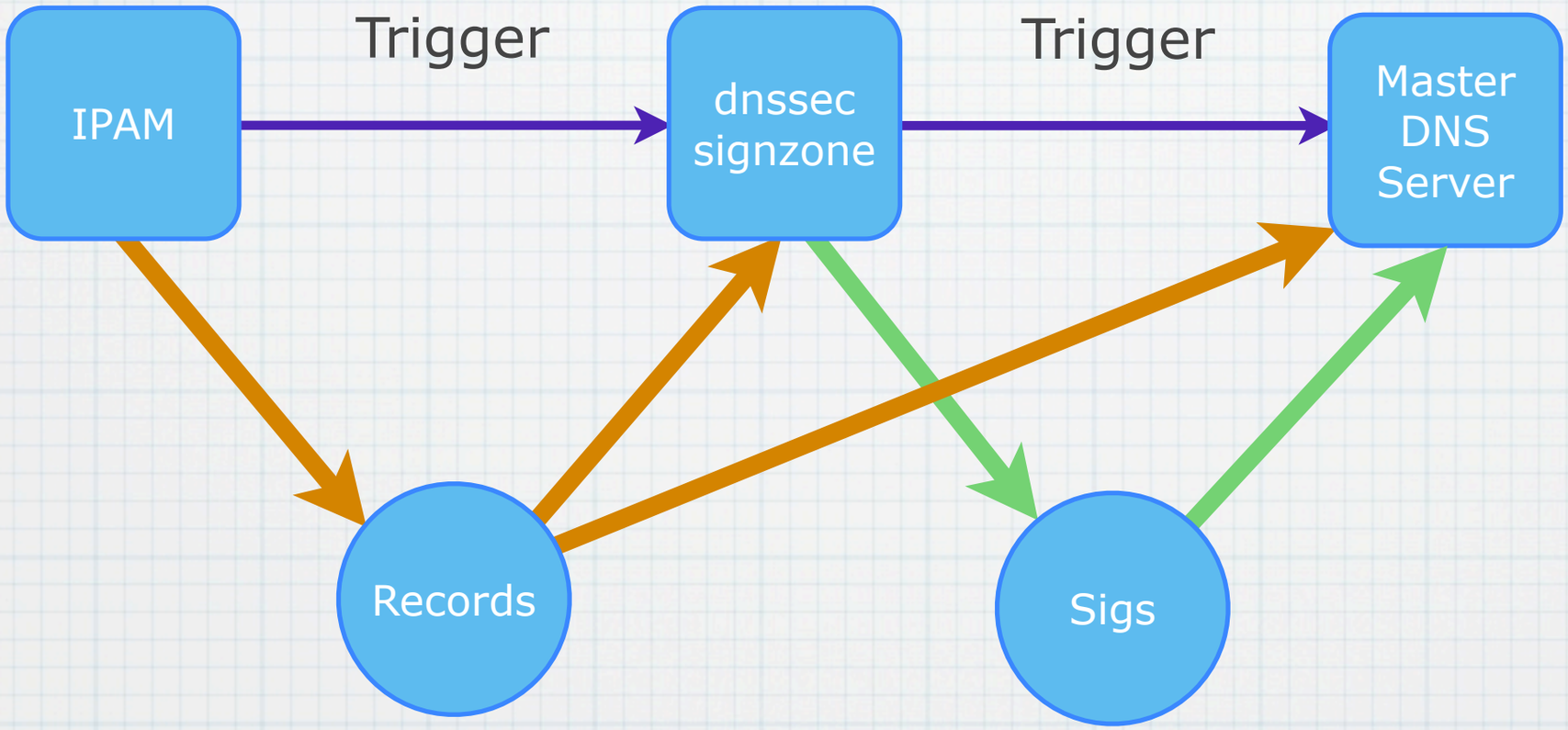
Copyright (c) 2011 Internet Systems Consortium

First Signing



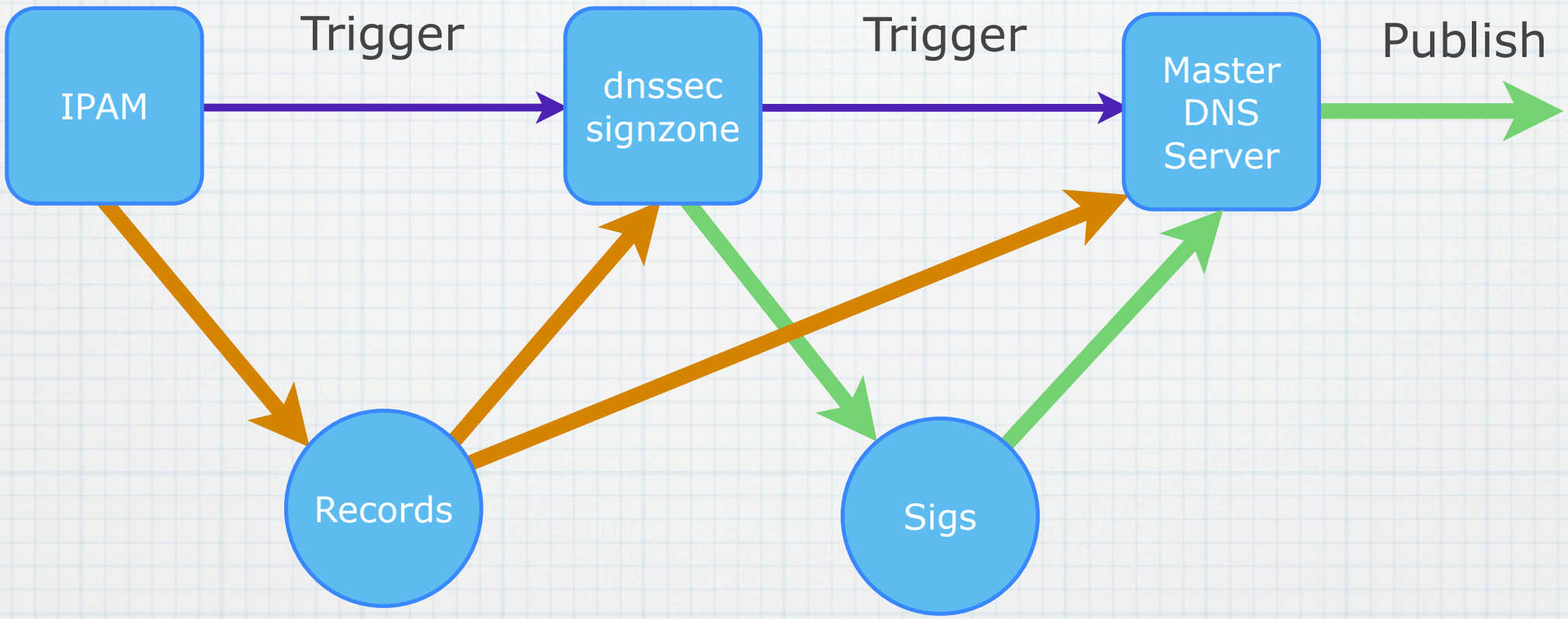
Copyright (c) 2011 Internet Systems Consortium

First Signing



Copyright (c) 2011 Internet Systems Consortium

First Signing

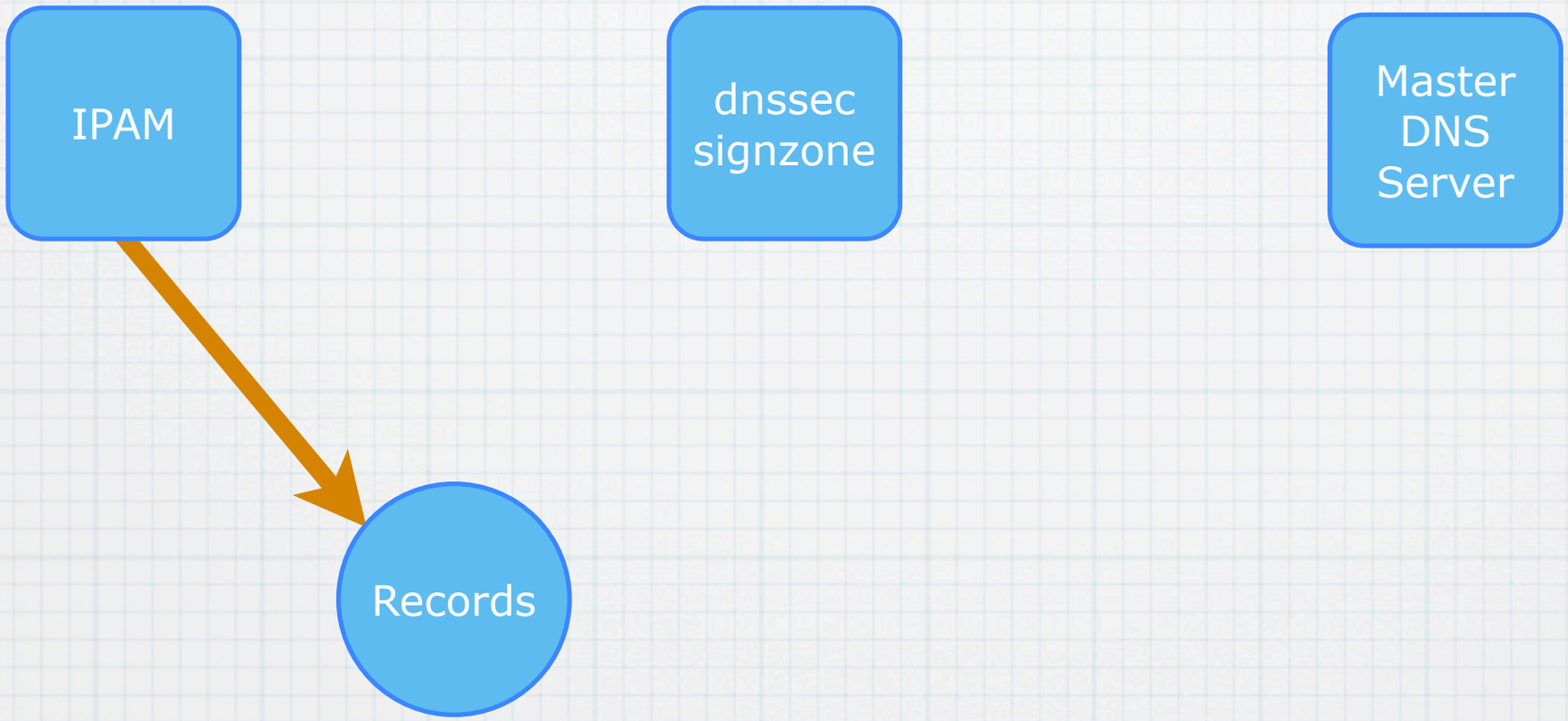


Copyright (c) 2011 Internet Systems Consortium

Subsequent Signing

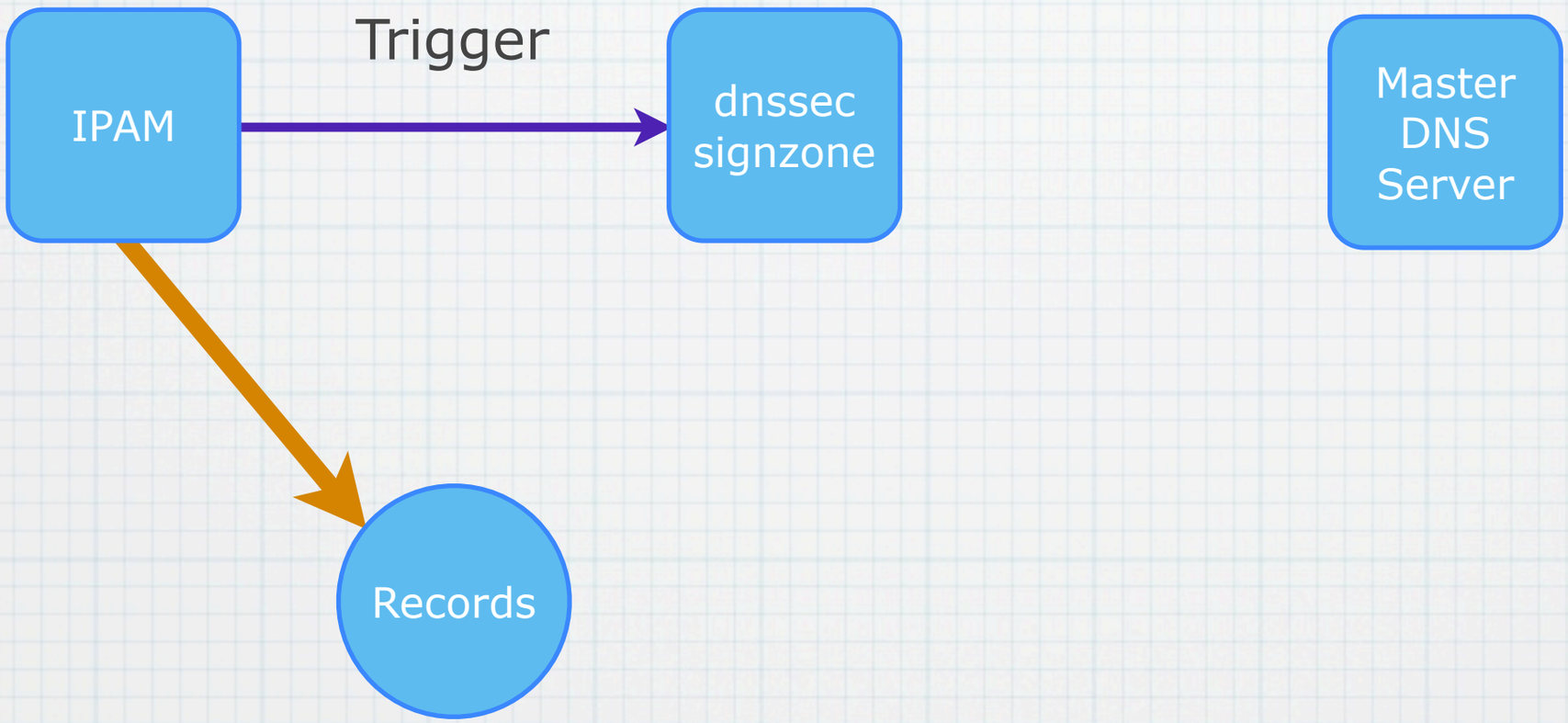
Copyright (c) 2011 Internet Systems Consortium

Subsequent Signing



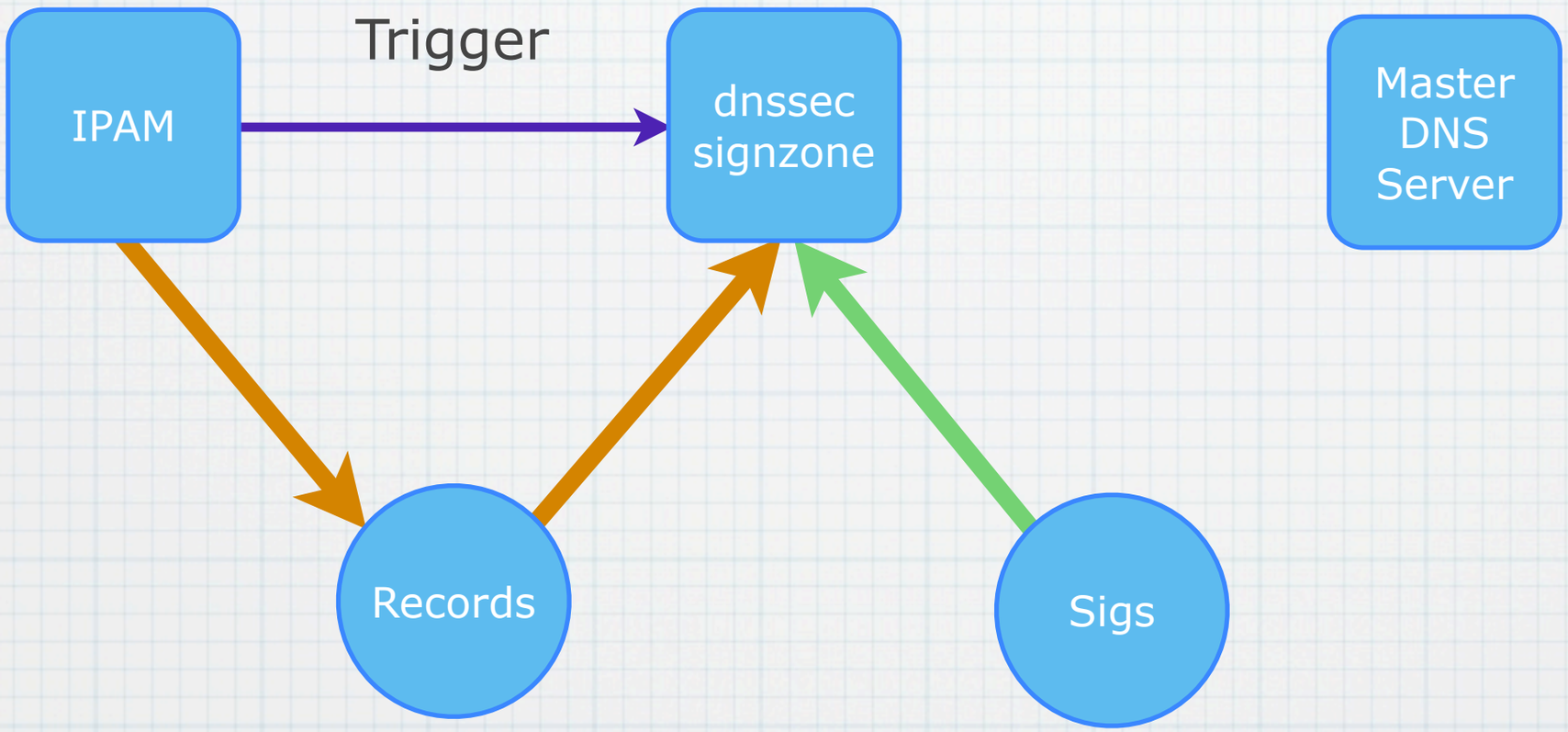
Copyright (c) 2011 Internet Systems Consortium

Subsequent Signing



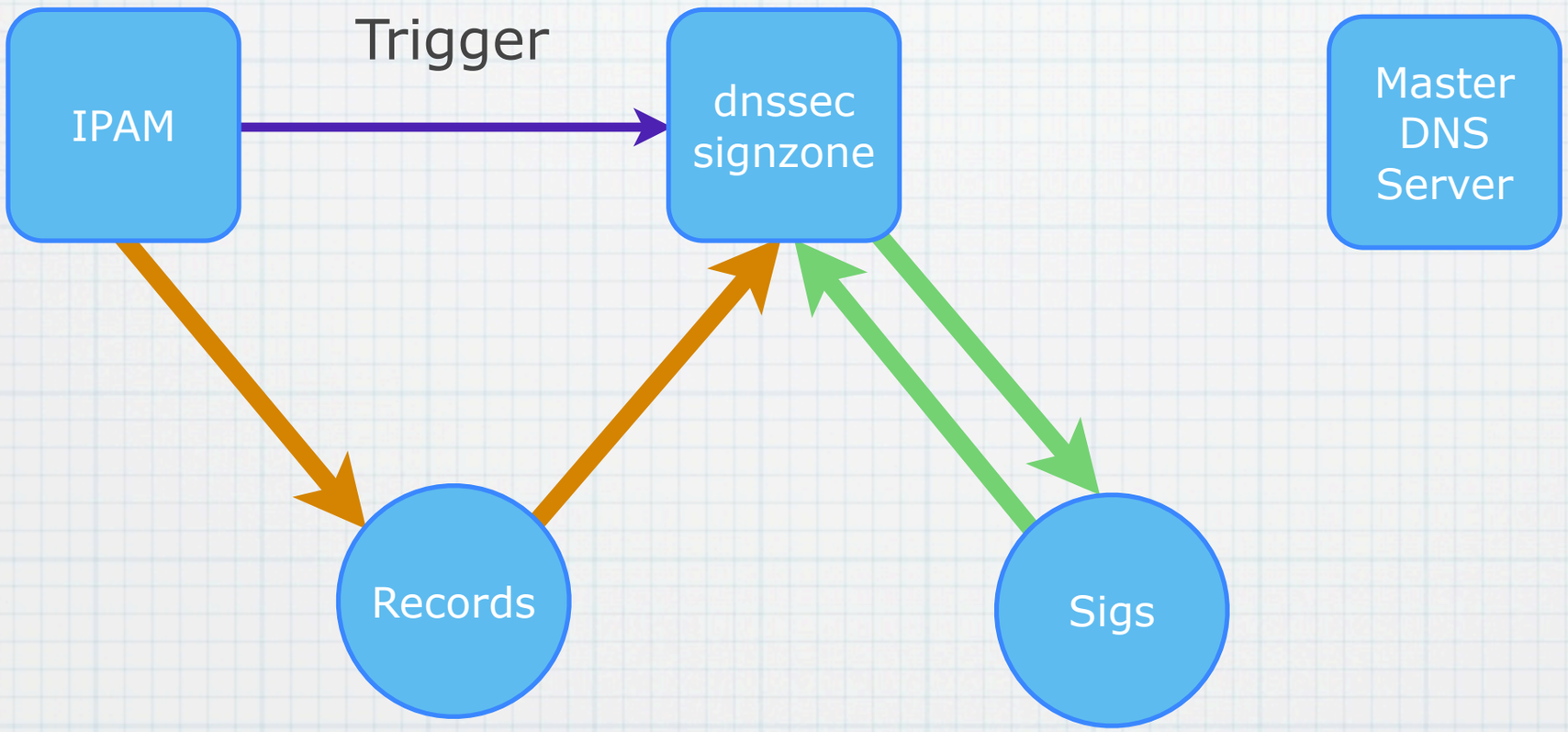
Copyright (c) 2011 Internet Systems Consortium

Subsequent Signing



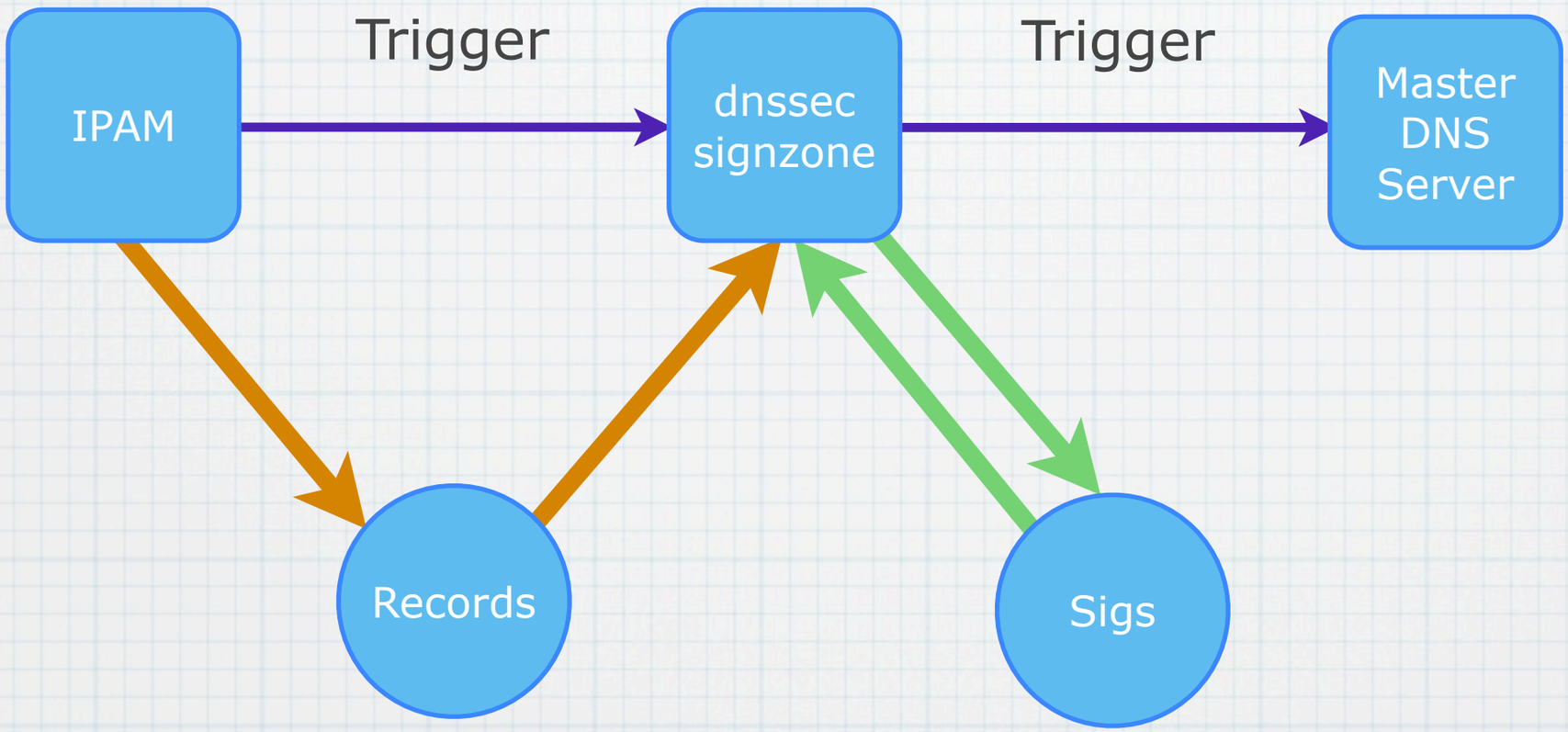
Copyright (c) 2011 Internet Systems Consortium

Subsequent Signing



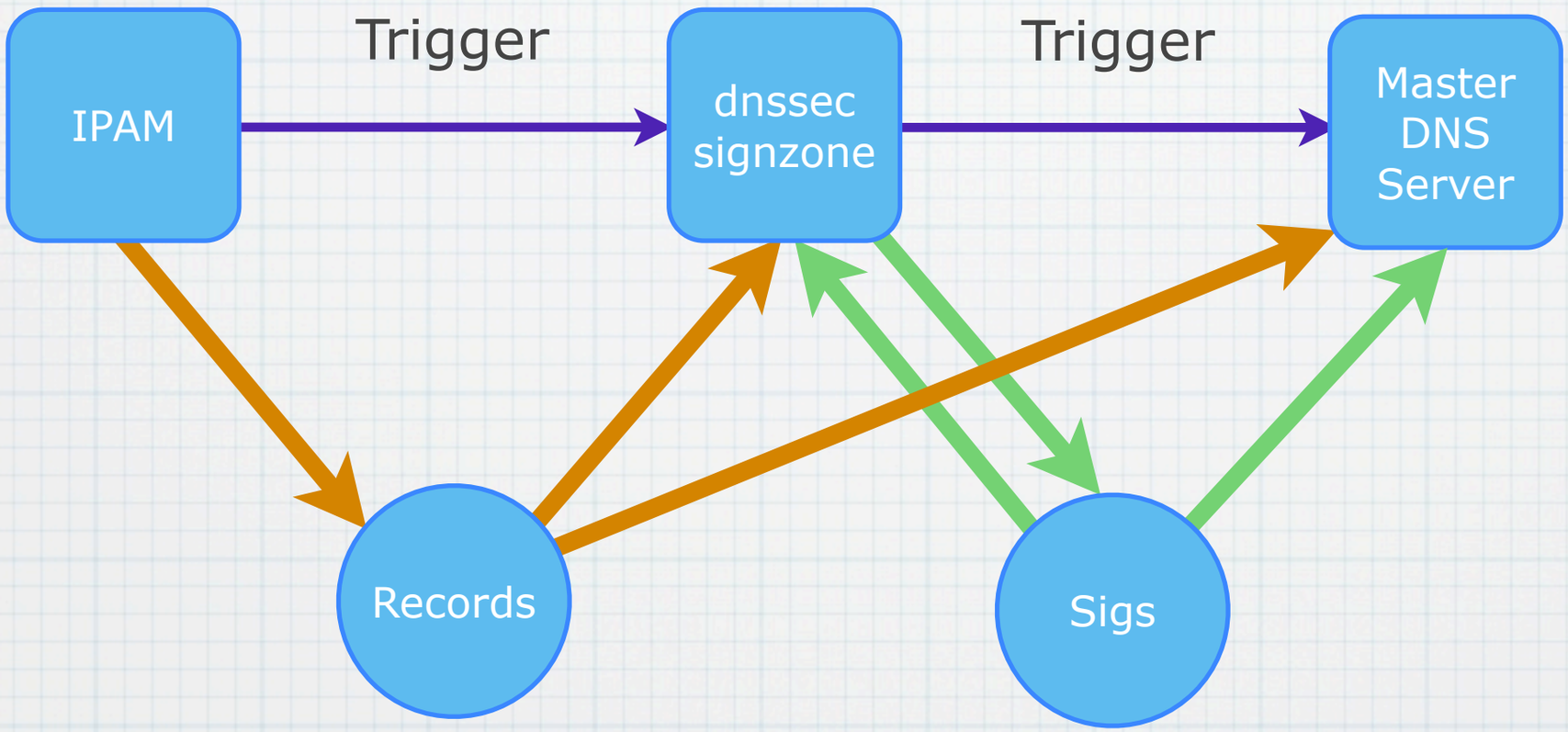
Copyright (c) 2011 Internet Systems Consortium

Subsequent Signing



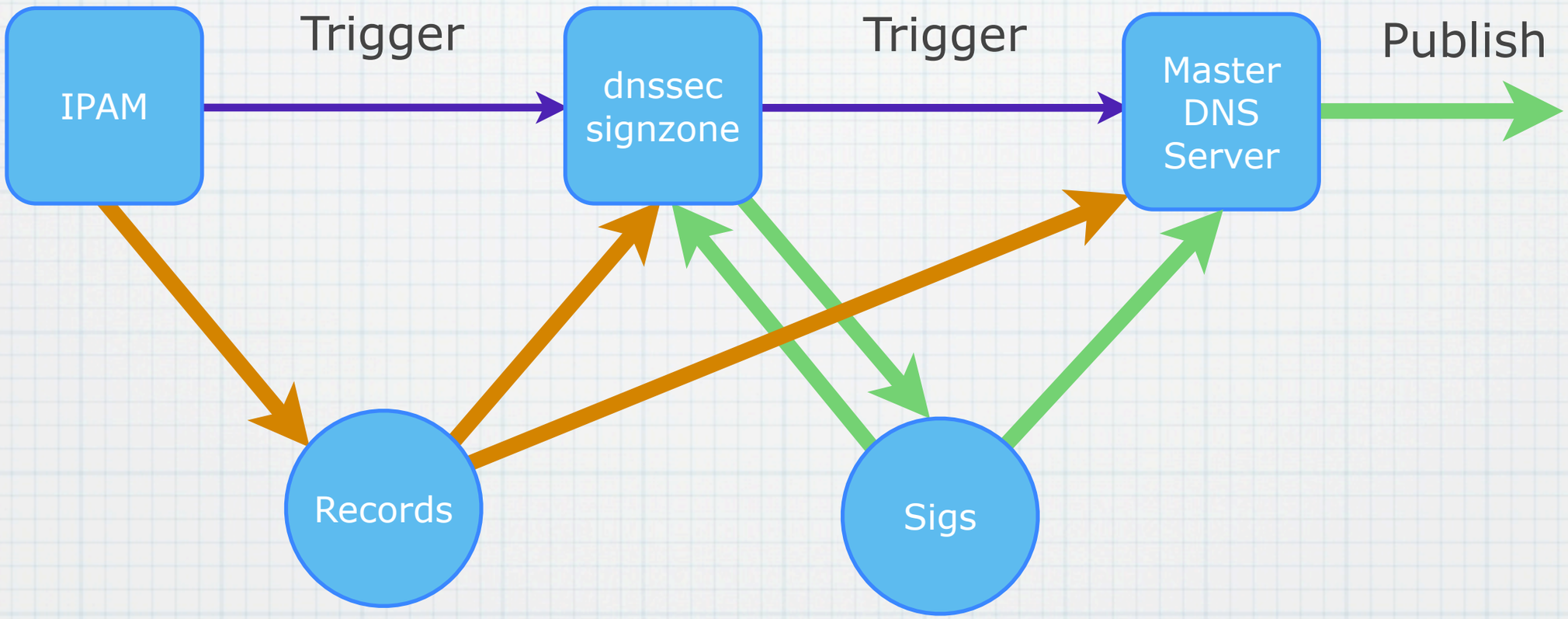
Copyright (c) 2011 Internet Systems Consortium

Subsequent Signing



Copyright (c) 2011 Internet Systems Consortium

Subsequent Signing



Copyright (c) 2011 Internet Systems Consortium

Using Stand-Aside Signing

Copyright (c) 2011 Internet Systems Consortium

Using Stand-Aside Signing

- Enable `ixfr-from-differences` on master

Copyright (c) 2011 Internet Systems Consortium

Using Stand-Aside Signing

- Enable `ixfr-from-differences` on master
- Enable IXFR on master and slaves

Copyright (c) 2011 Internet Systems Consortium

Using Stand-Aside Signing

- Enable `ixfr-from-differences` on master
- Enable IXFR on master and slaves
- Alter signing scripts

Copyright (c) 2011 Internet Systems Consortium

Stand-Aside Signing

Copyright (c) 2011 Internet Systems Consortium

Inline Signing Benefits

Copyright (c) 2011 Internet Systems Consortium

Inline Signing Benefits

- Deploying DNSSEC

Copyright (c) 2011 Internet Systems Consortium

Inline Signing Benefits

- Deploying DNSSEC
- IPAM or other source

Copyright (c) 2011 Internet Systems Consortium

Inline Signing Benefits

- Deploying DNSSEC
- IPAM or other source
- Minimize cost

Copyright (c) 2011 Internet Systems Consortium

Inline Signing Benefits

- Deploying DNSSEC
- IPAM or other source
- Minimize cost
- Minimize operational changes

Copyright (c) 2011 Internet Systems Consortium

Inline Signing Benefits

- Deploying DNSSEC
- IPAM or other source
- Minimize cost
- Minimize operational changes
- Parallel production and testbed

Copyright (c) 2011 Internet Systems Consortium

Inline Signing Benefits

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

Copyright (c) 2011 Internet Systems Consortium

Hidden Master

Copyright (c) 2011 Internet Systems Consortium

Hidden Master

- Master server receives updates, and notifies slaves of changes.

Copyright (c) 2011 Internet Systems Consortium

Hidden Master

- Master server receives updates, and notifies slaves of changes.
- Slave transfer from the master using AXFR and IXFR.

Copyright (c) 2011 Internet Systems Consortium

Hidden Master

- 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.

Copyright (c) 2011 Internet Systems Consortium

Hidden Master

Copyright (c) 2011 Internet Systems Consortium

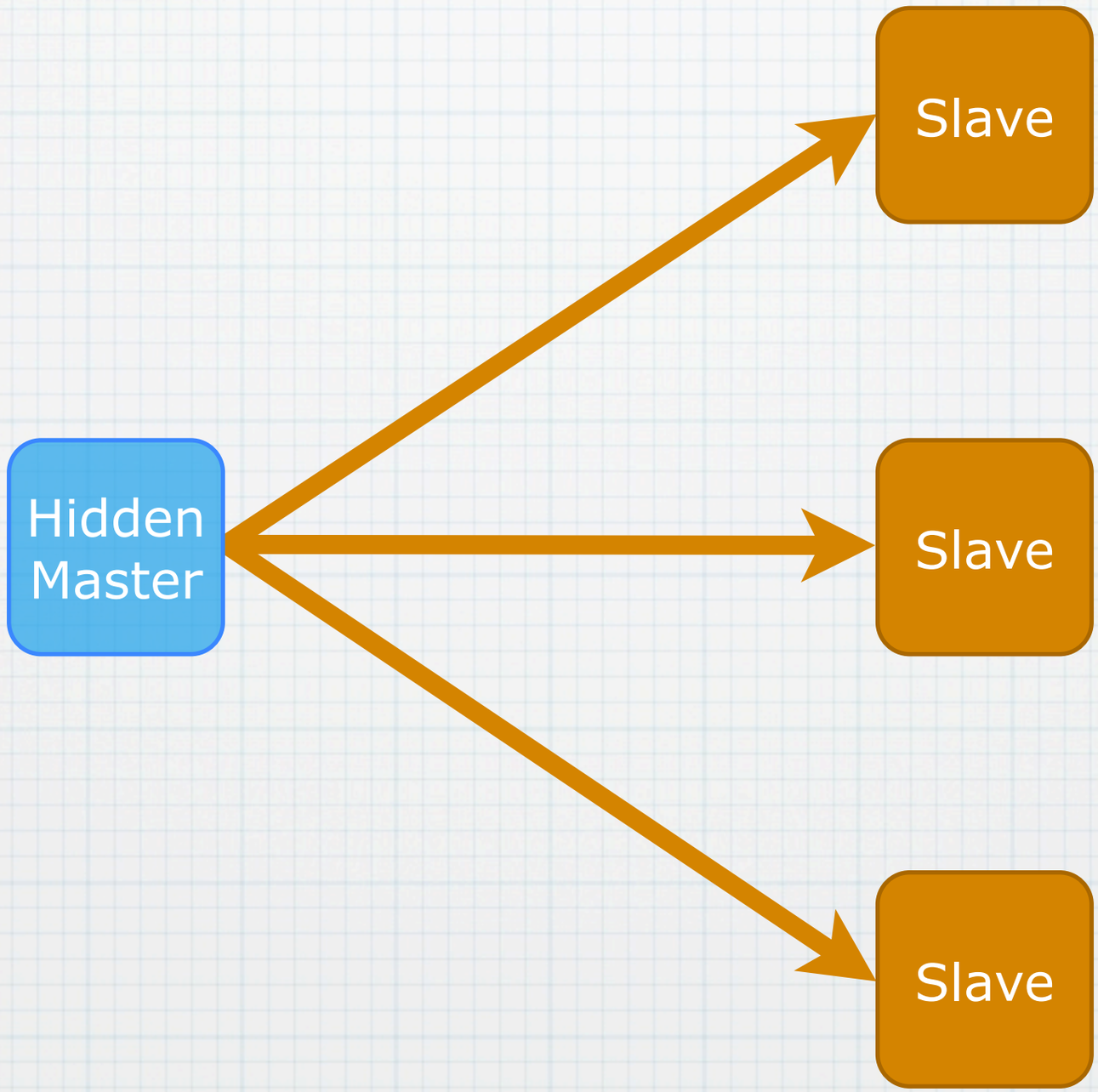
Hidden Master

Copyright (c) 2011 Internet Systems Consortium

Hidden Master

Copyright (c) 2011 Internet Systems Consortium

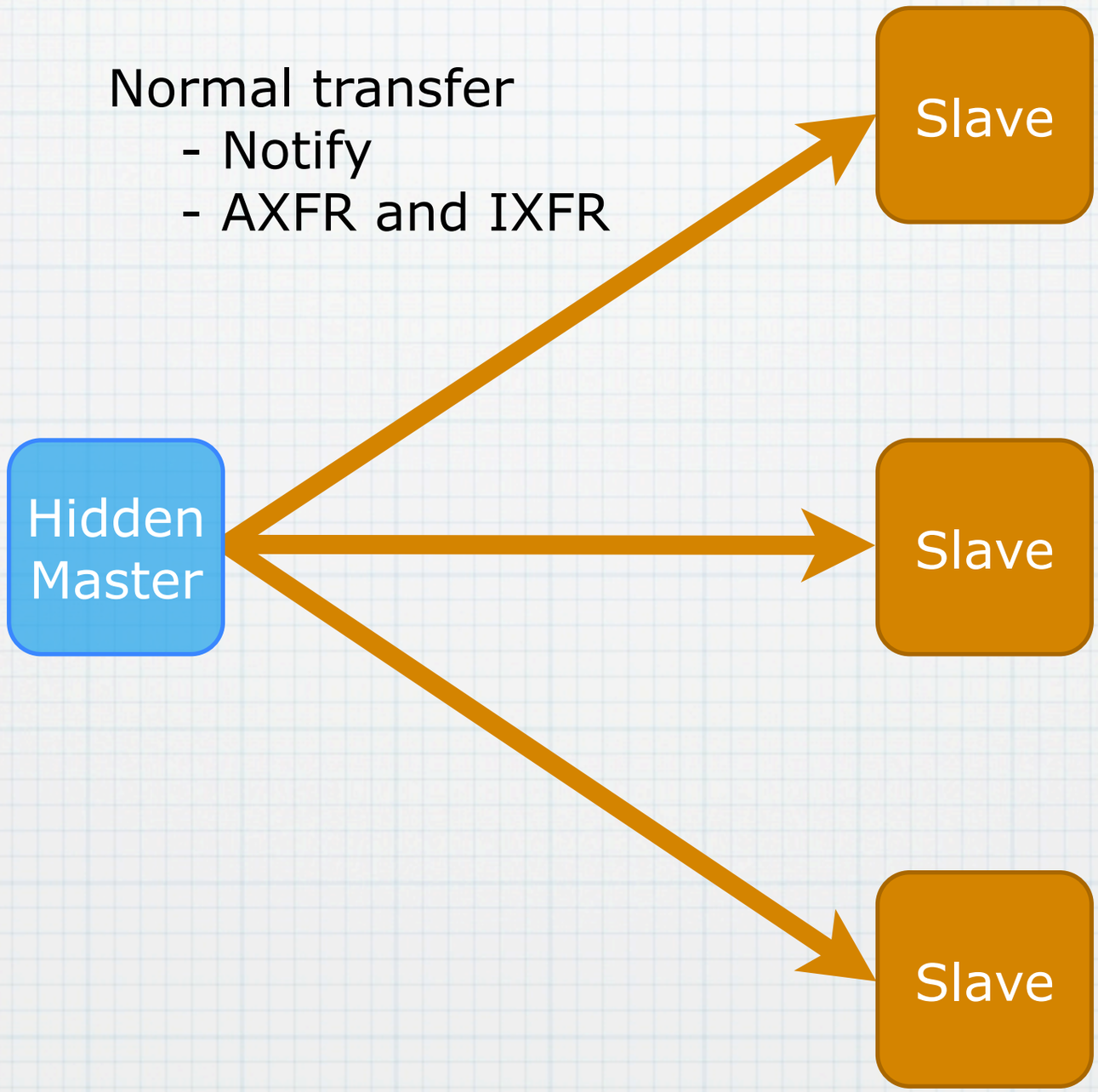
Hidden Master



Copyright (c) 2011 Internet Systems Consortium

Hidden Master

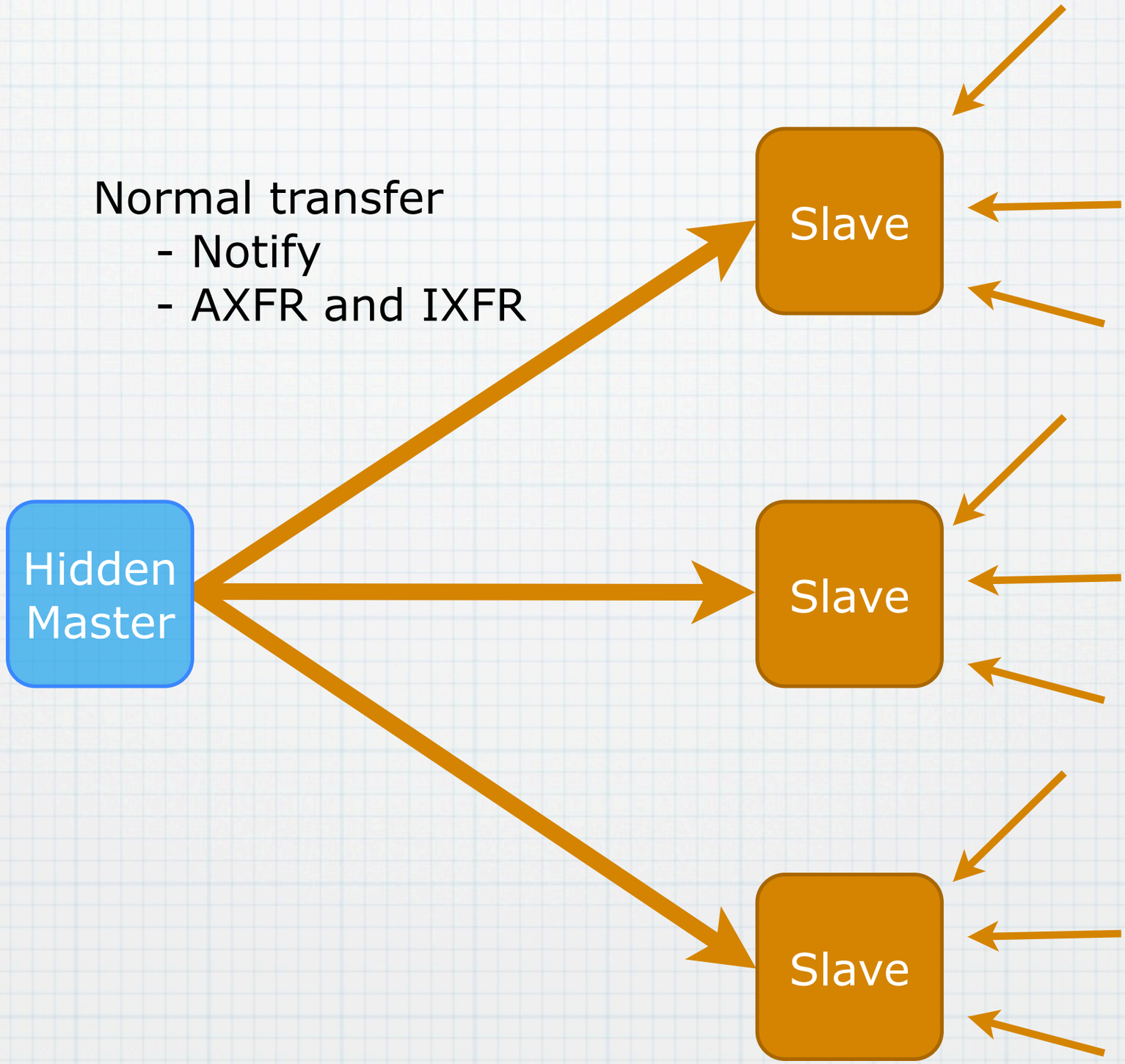
Normal transfer
- Notify
- AXFR and IXFR



Copyright (c) 2011 Internet Systems Consortium

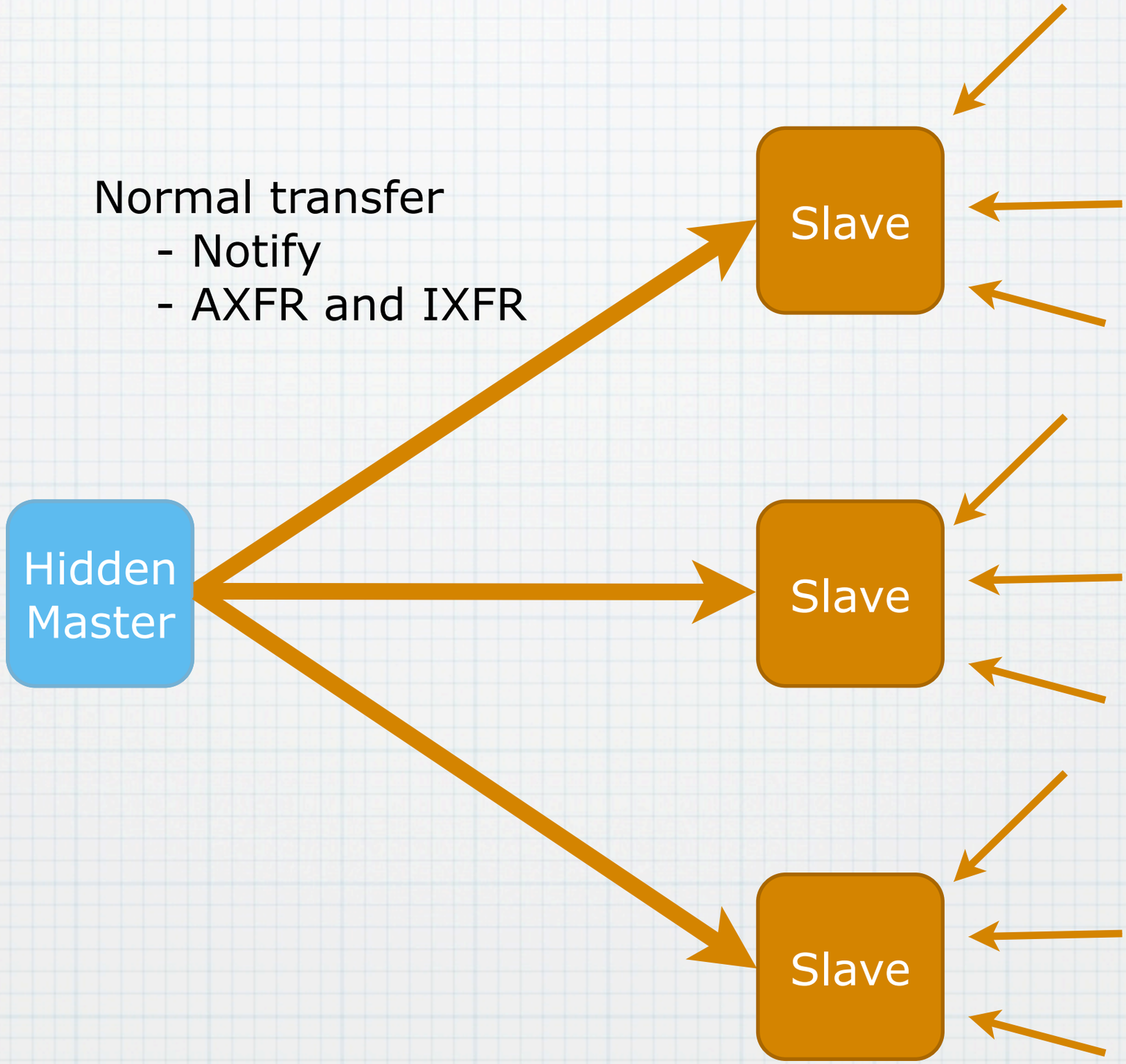
Hidden Master

Normal transfer
- Notify
- AXFR and IXFR



Copyright (c) 2011 Internet Systems Consortium

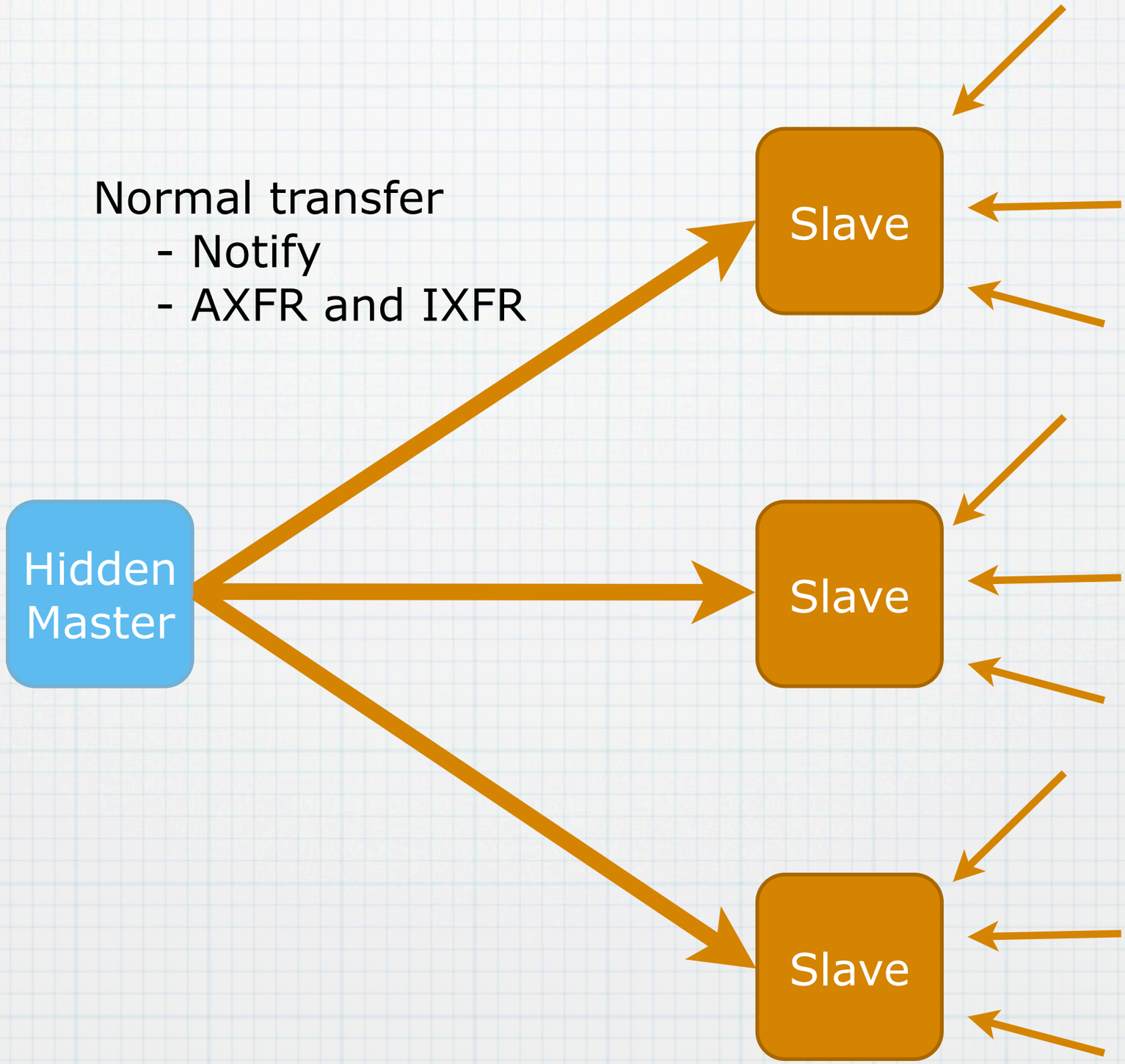
Normal transfer
- Notify
- AXFR and IXFR



Copyright (c) 2011 Internet Systems Consortium

Hidden Master + Inline Signing

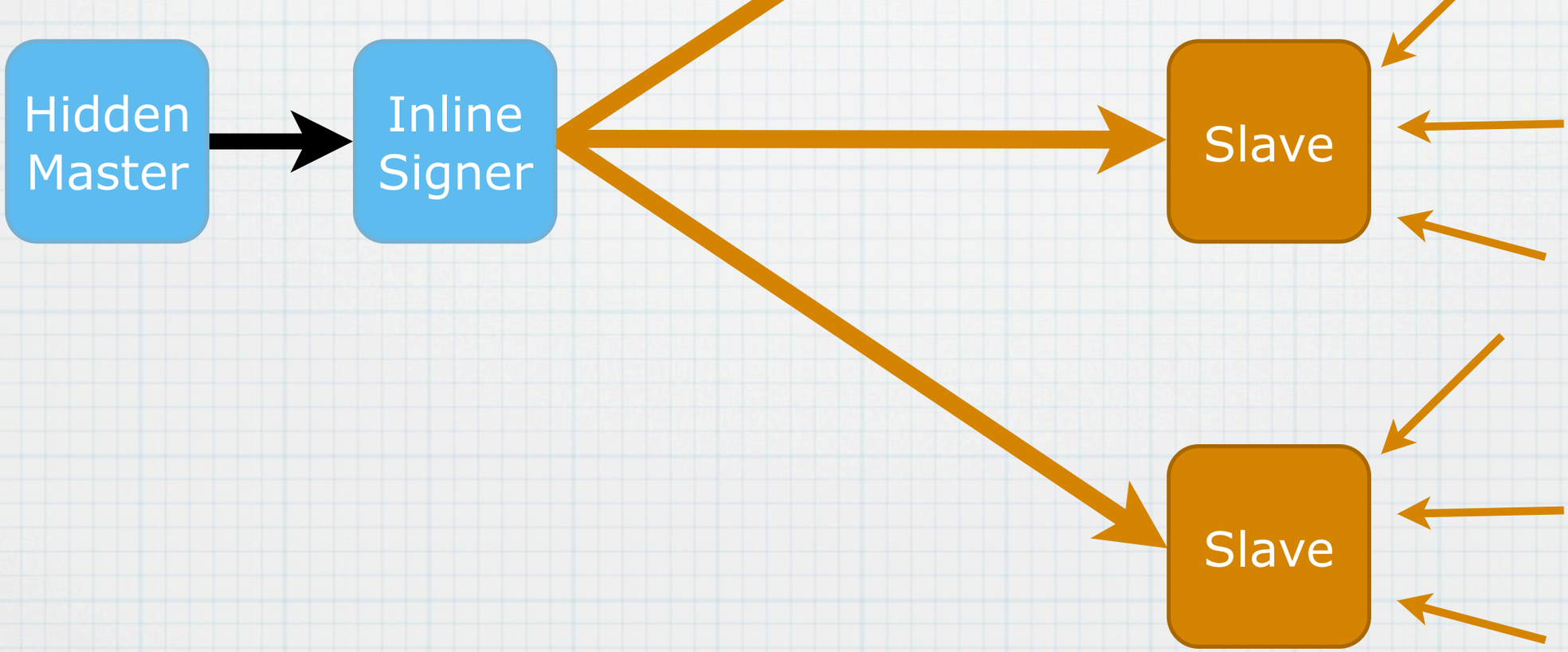
Normal transfer
- Notify
- AXFR and IXFR



Copyright (c) 2011 Internet Systems Consortium

Hidden Master + Inline Signing

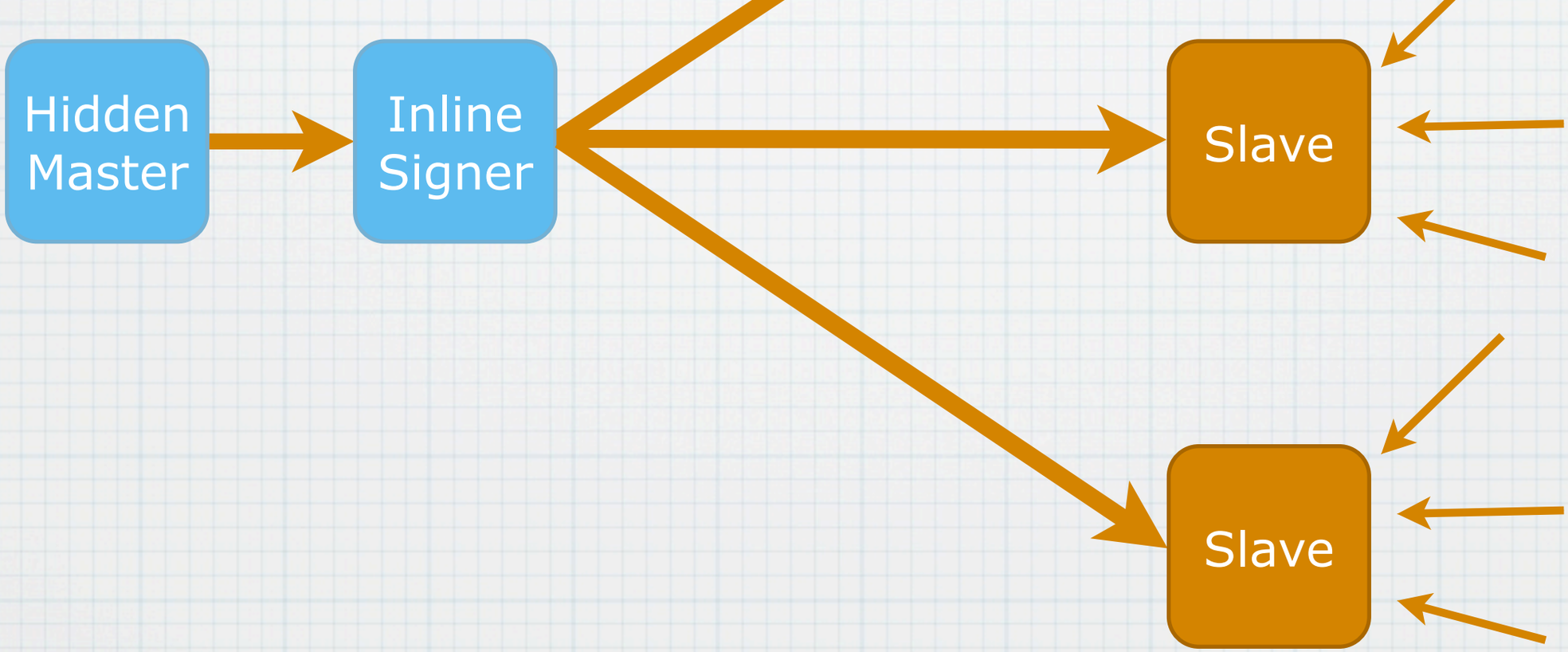
Normal transfer
- Notify
- AXFR and IXFR



Copyright (c) 2011 Internet Systems Consortium

Hidden Master + Inline Signing

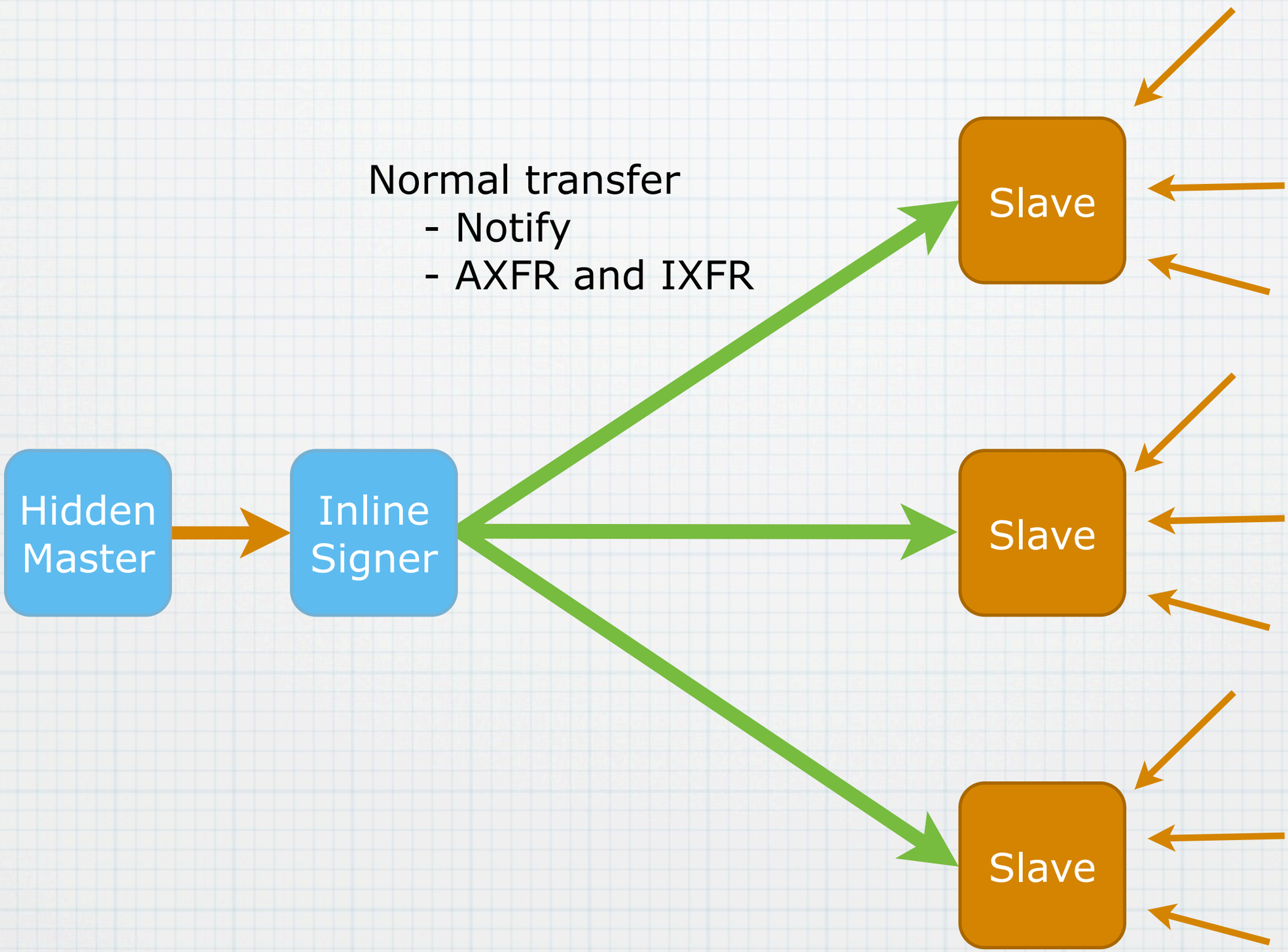
Normal transfer
- Notify
- AXFR and IXFR



Copyright (c) 2011 Internet Systems Consortium

Hidden Master + Inline Signing

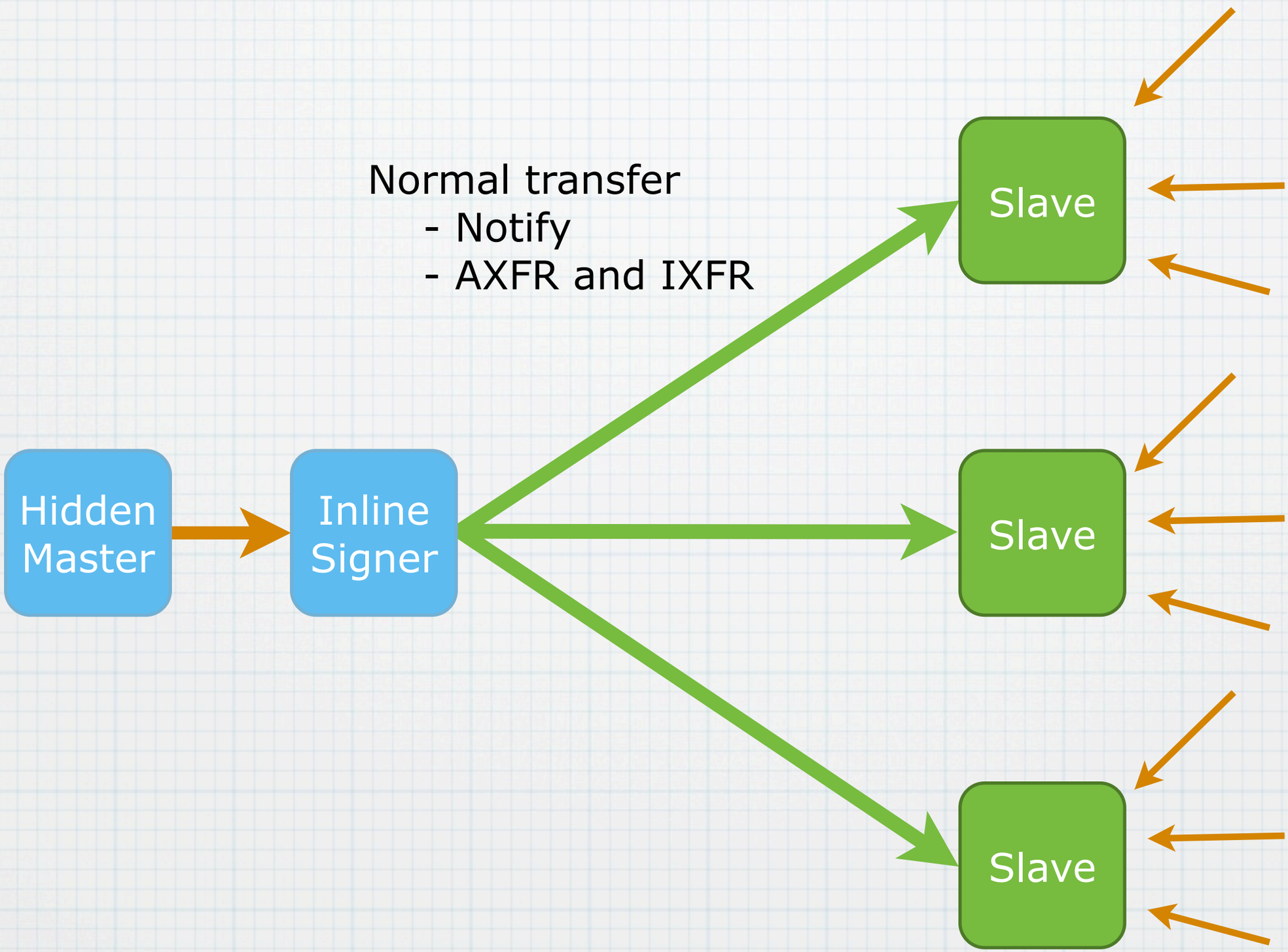
Normal transfer
- Notify
- AXFR and IXFR



Copyright (c) 2011 Internet Systems Consortium

Hidden Master + Inline Signing

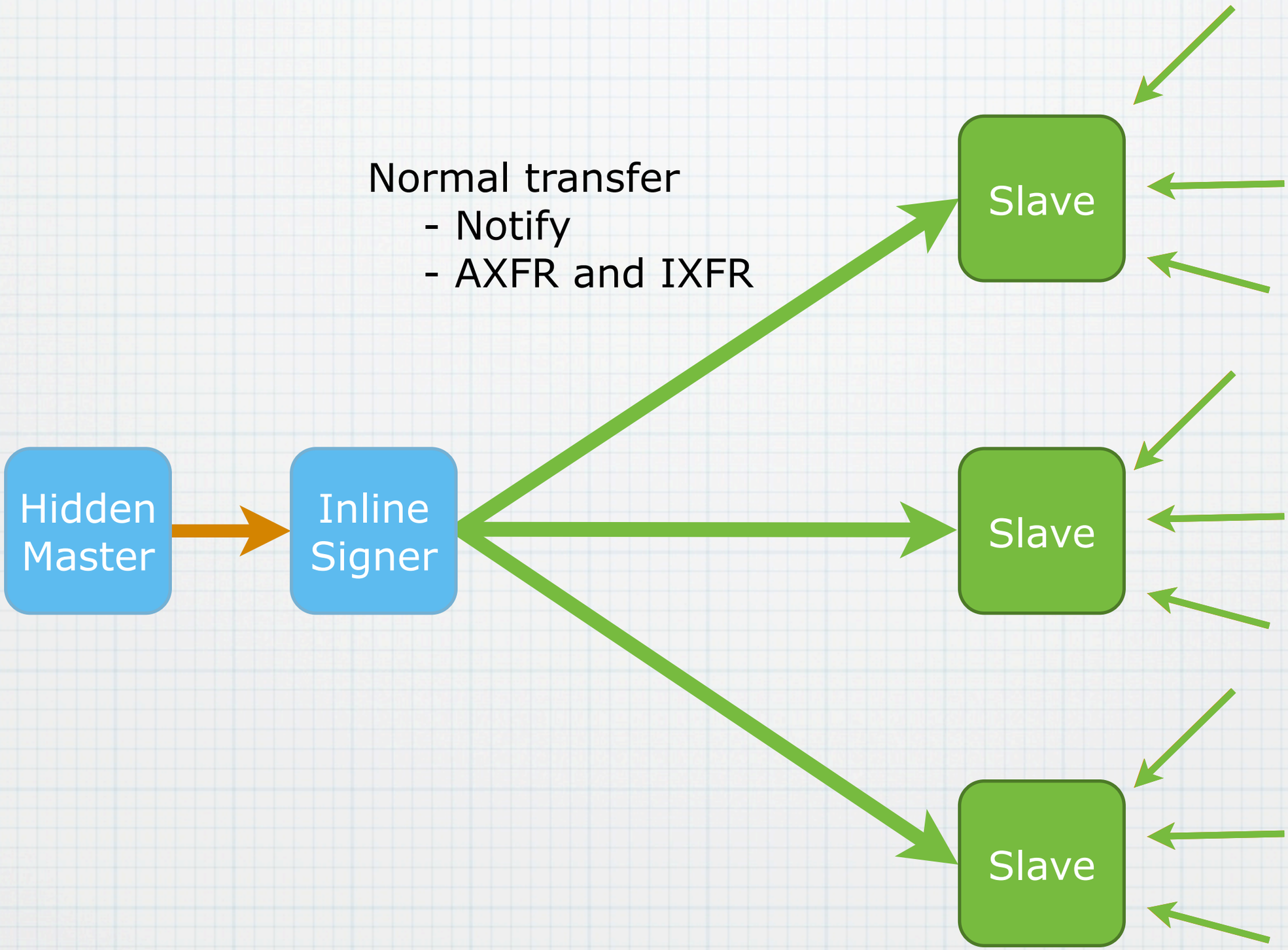
Normal transfer
- Notify
- AXFR and IXFR



Copyright (c) 2011 Internet Systems Consortium

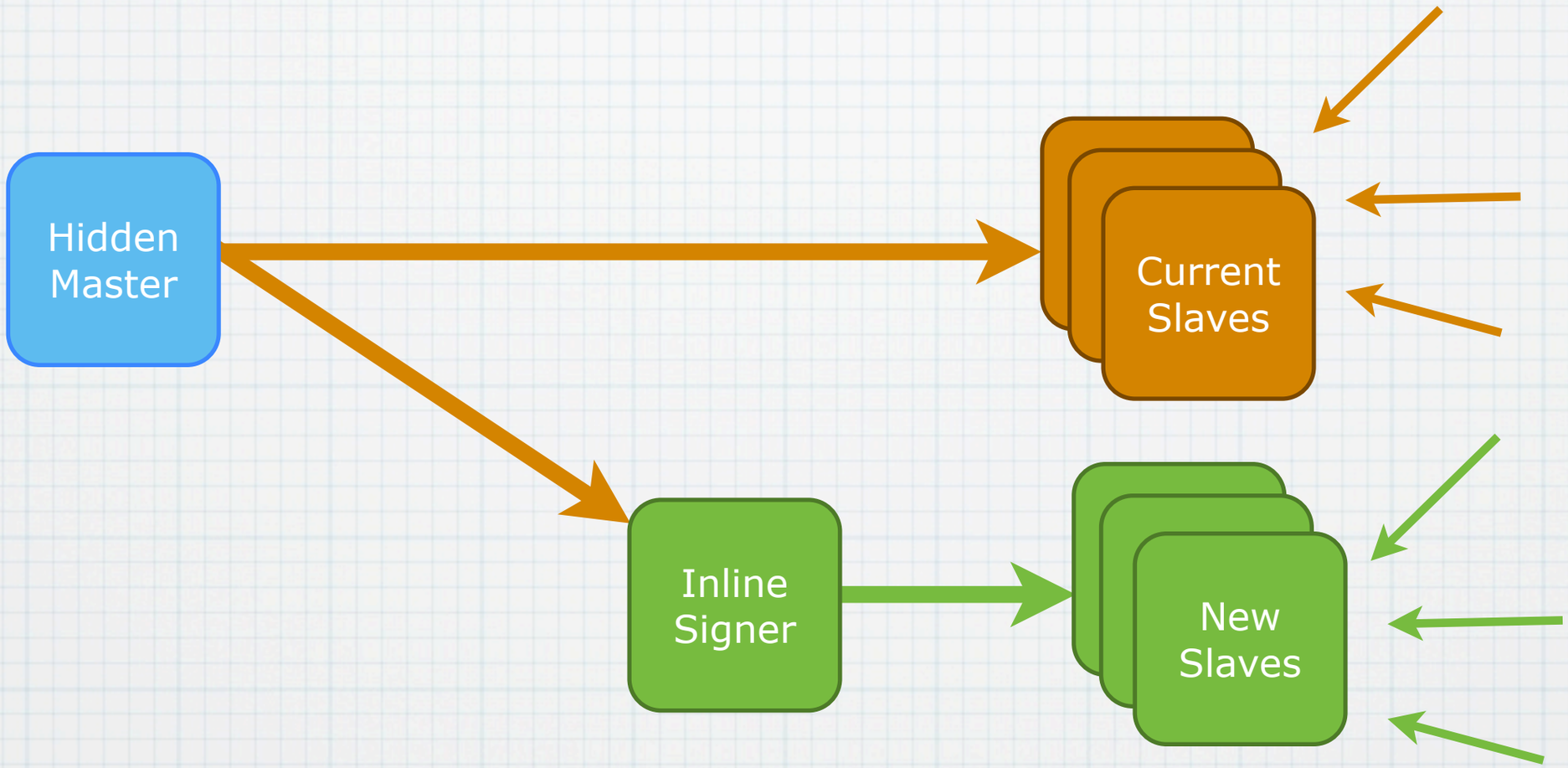
Hidden Master + Inline Signing

Normal transfer
- Notify
- AXFR and IXFR



Copyright (c) 2011 Internet Systems Consortium

Inline Signing + Minimal Risk



Copyright (c) 2011 Internet Systems Consortium

Upcoming Presentation

Watch our upcoming presentation on Inline Signing!

http://www.isc.org/webinars

Copyright (c) 2011 Internet Systems Consortium

Gimme!

- Released planned for December 13, 2011
  - Forum release about one week earlier
- Alpha and Beta before then
- Sign up for the `bind-announce` list to receive release notifications

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

Copyright (c) 2011 Internet Systems Consortium

Copyright (c) 2011 Internet Systems Consortium

Upcoming Training

2012:

- 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

Copyright (c) 2011 Internet Systems Consortium

Upcoming Web Seminars

Next Week: December 7th, 2011

Update for CVE 2011-4313 and ISC Security Vulnerability Disclosure Policy.

Customers, Forum Members, and special guests.

If you wish to attend, please contact sales@isc.org to request an invitation, or your account manager if you are currently a customer.

To be announced for 2012:

- Registry Service
- Training Certification
- Product Updates
- Inline Signing
- Anycast

Copyright (c) 2011 Internet Systems Consortium

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 2012Q1 training sessions offered by ISC. 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.

Copyright (c) 2011 Internet Systems Consortium

Keeping in Contact

http://www.facebook.com/InternetSystemsConsortium

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

http://twitter.com/ISCdotORG

Copyright (c) 2011 Internet Systems Consortium

ISC Resources

Knowledge Base for many things

http://deepthought.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

Copyright (c) 2011 Internet Systems Consortium

Thank you for your time.

www.isc.org

Copyright (c) 2011 Internet Systems Consortium