The Wild Card Incident of 9/15/2003

Steve Crocker Chair

Security and Stability Advisory Committee

Primary Security and Stability ICANN Components

- Constituent Participatory Organizations
  - Generic Names Supporting Organization
  - Country Code Names Supporting Organization
  - Government Advisory Council
    - 80 countries and 5 treaty organizations
  - Root Server Advisory Committee
- Specialist Groups
  - IANA
    - Administers root database and address allocation
  - Security and Stability Advisory Committee
    - Volunteer experts on security and stability issues

SECSAC Committee

- **Steve Crocker, Chair**
- **Alain Patrick Aina**
- **Jaap Akkerhuis**
- **Doug Barton**
- **Steven M. Bellovin**
- **Rob Blokzijl**
- **David R. Conrad**
- **Johan Ihren**
- **Mark Kosters**
- **Allison Mankin**

- **Ram Mohan**
- **Russ Mundy**
- **Jun Murai**
- **Frederico A.C. Neves**
- **Ray Plzak**
- **Doron Shikmoni**
- **Ken Silva**
- **Bruce Tonkin**
- **Paul Vixie**
- **Rick Wesson**

Staff support: Jim Galvin

SECSAC Committee Strengths

- Root Server Operators
- gTLD Operators
- ccTLD Operators
- Name Space Registries
- Regional Internet Registries (RIRs)
- Registrars
- Internet Security

No policy or political members(!)

Preamble

- On Sept 15, VeriSign introduced change to .com and .net domain
- Redirected unassigned names to their own server (SiteFinder)
- Immediate complaints and problem reports
- Several actions, including SECSAC

SECSAC Involvement

- Advisory issued 9/22
- Public inputs
  - secsac-comment@icann.org
- Public meetings 10/7 & 10/15
- More public inputs
- Report will come toward end of November

SECSAC in the larger process

- SECSAC is an advisory committee
    - We only speak. We don't decide or enforce. Others may choose to listen.
    - ICANN management will deliberate and choose path following our report.
- Focus on Security and Stability
    - Not competition, etc.
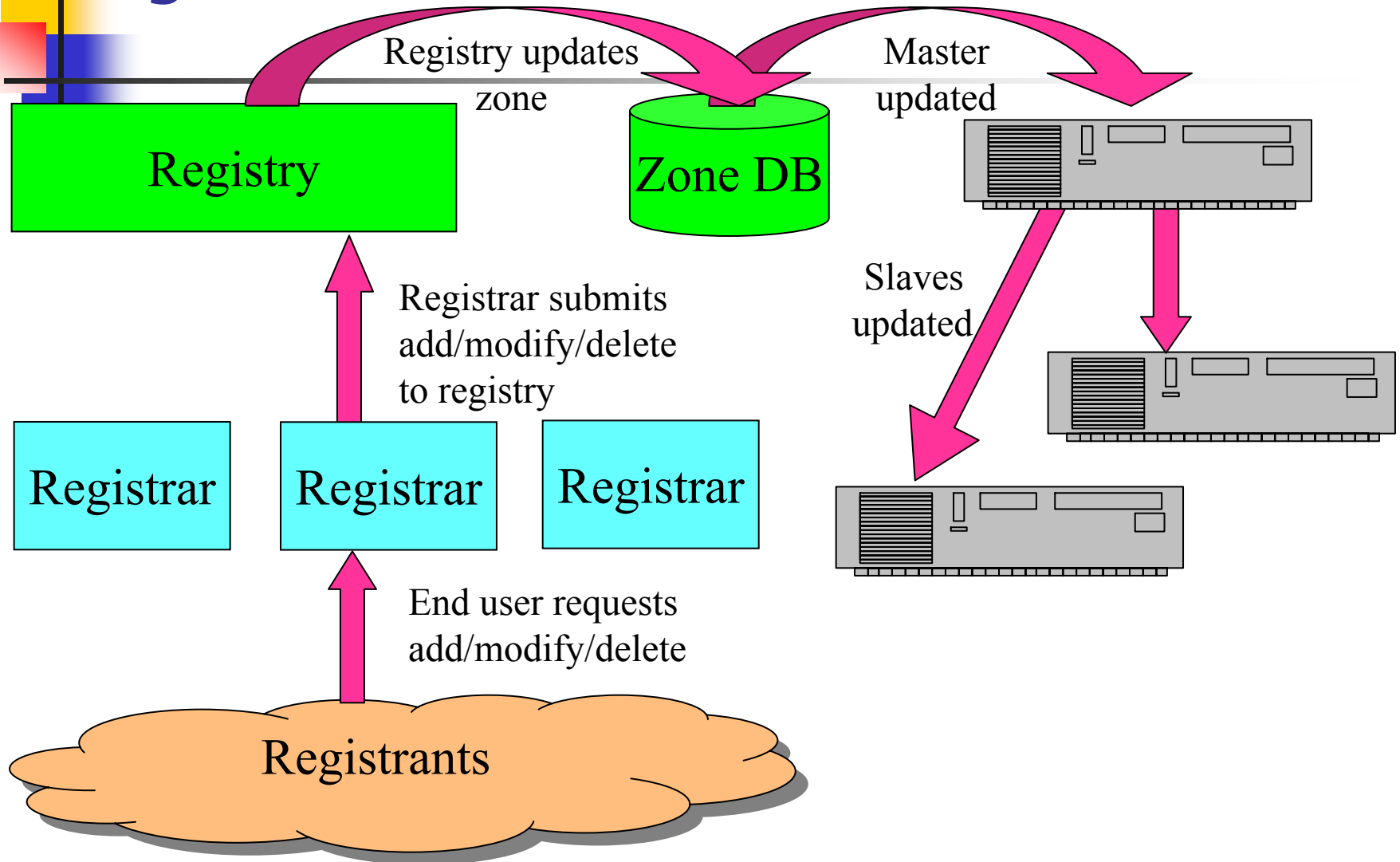   - But may include large issues

What Happened

- VeriSign used the wild card feature to redirect all uninstantiated names to their own servers
    - Previously, returned standard error code
    - This was a <u>change</u> to an existing service
- Some things broke
- Some took defensive action

Registries, Registrars, and Registrants

Registry updates zone

Master updated

Registry

Zone DB

Registrar submits add/modify/delete to registry

Slaves updated

Registrar

Registrar

Registrar

End user requests add/modify/delete

Registrants

Name Resolution

- *Name resolution* is the process by which resolvers and name servers cooperate to find data in the name space
- To find information anywhere in the name space, a name server only needs the names and IP addresses of the name servers for the root zone (the "root name servers")

Name Resolution

- A name server receiving a query from a resolver looks for the answer in its authoritative data first and then in its cache

  - If it doesn't have the requested data and is not authoritative for the domain in the query, other servers must be consulted

Name Resolution Example
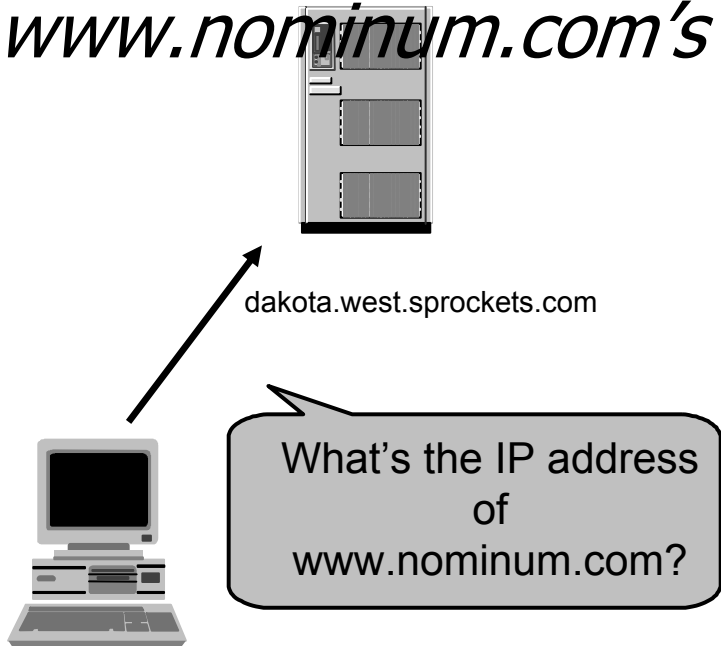
- Let's look at the resolution process step-by-step:

annie.west.sprockets.com

```
ping www.nominum.com.
```

Name Resolution Example

The workstation *annie* asks its configured name server, *dakota,* for *www.nominum.com's* address
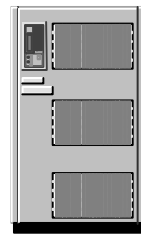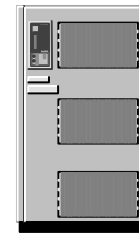
dakota.west.sprockets.com

What's the IP address of www.nominum.com?

annie.west.sprockets.com

```
ping www.nominum.com.
```

Name Resolution Example

The name server *dakota* asks a root name server, *m*, for *www.nominum.com's* address

dakota.west.sprockets.com

m.root-servers.net

What's the IP address of www.nominum.com?
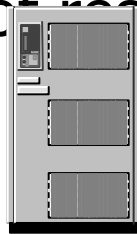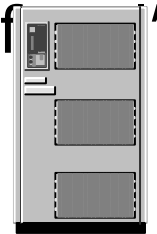
annie.west.sprockets.com

`ping www.nominum.com.`

Name Resolution Example

- The root server *m* refers *dakota* to the *com* name servers
- This type of response is called a "referral"

dakota.west.sprockets.com

m.root-servers.net

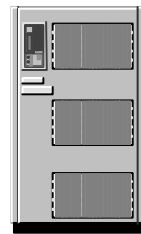Here's a list of the com name servers. Ask one of them.

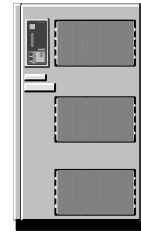annie.west.sprockets.com

`ping www.nominum.com.`

Name Resolution Example

The name server *dakota* asks a *com* name server, *f*, for *www.nominum.com's* address

What's the IP address of www.nominum.com?
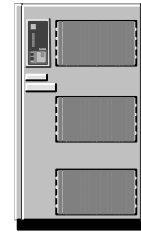
m.root-servers.net

dakota.west.sprockets.com

f.gtld-servers.net

annie.west.sprockets.com
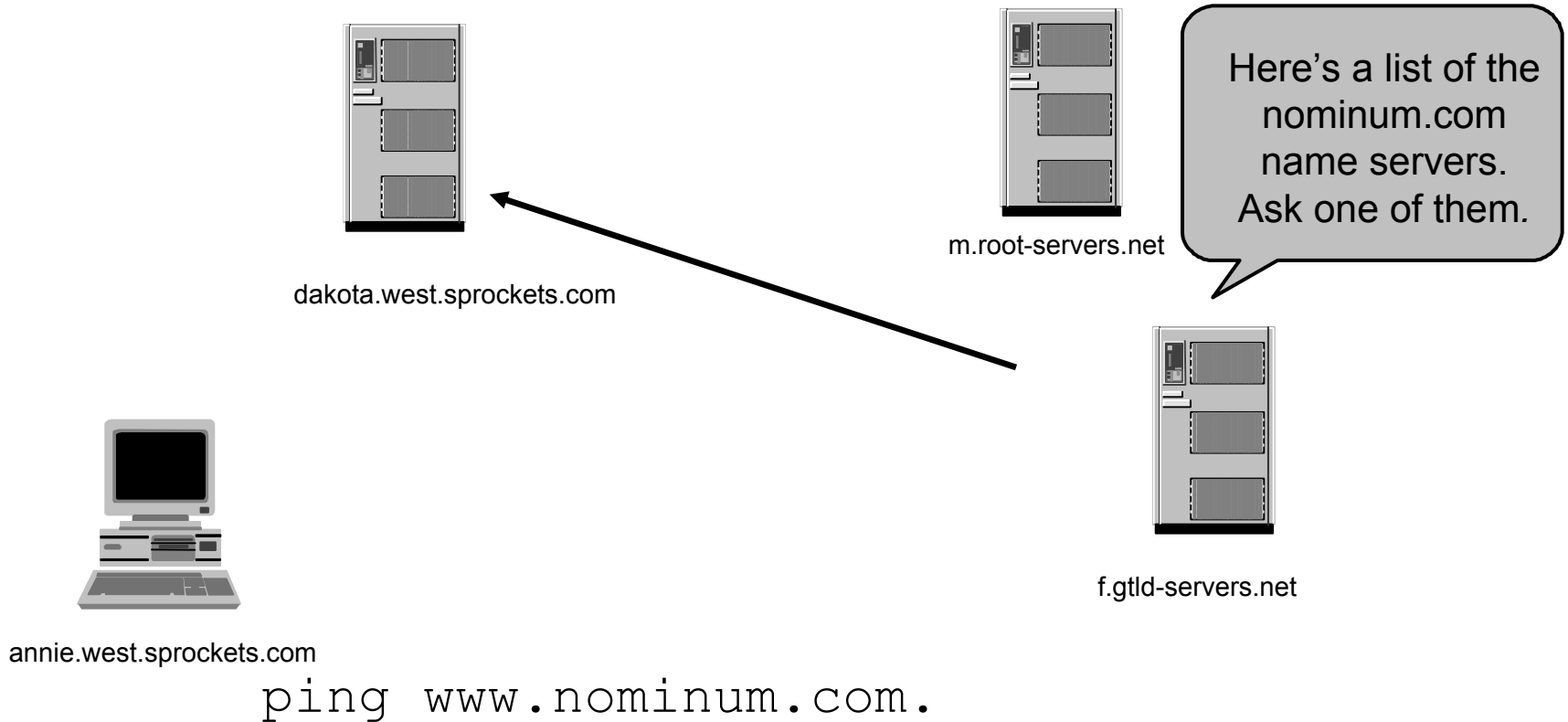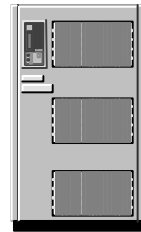
`ping www.nominum.com.`

Name Resolution Example

The *com* name server *f* refers *dakota* to the *nominum.com* name servers

dakota.west.sprockets.com

m.root-servers.net

Here's a list of the nominum.com name servers. Ask one of them.

f.gtld-servers.net

annie.west.sprockets.com

`ping www.nominum.com.`

If the Name doesn't exist

dakota.west.sprockets.com

m.root-servers.net

Here's the address of www.nnominum.com

f.gtld-servers.net
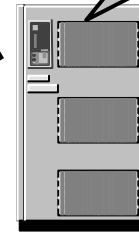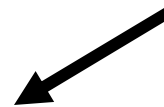
annie.west.sprockets.com
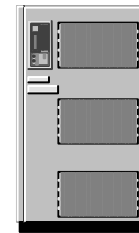
`ping www.nnominum.com.`

Name Resolution Example

The name server *dakota* asks a *nominum.com* name server, *ns1.sanjose*, for *www.nominum.com's* address

What's the IP address of www.nominum.com?

m.root-servers.net

dakota.west.sprockets.com

ns1.sanjose.nominum.net

f.gtld-servers.net
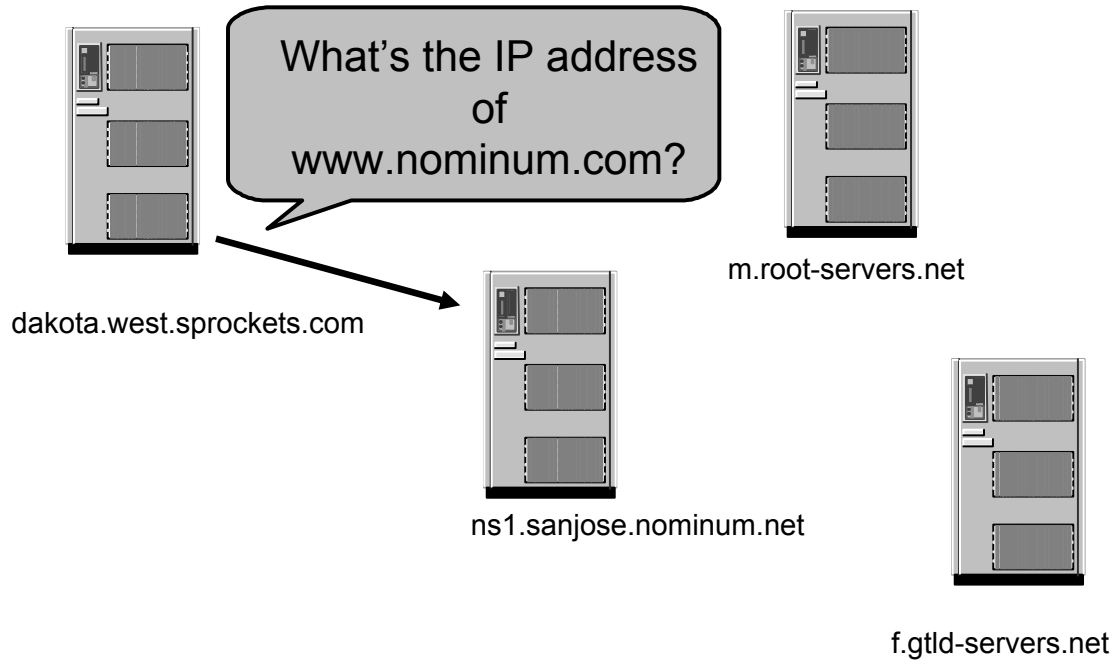
annie.west.sprockets.com

`ping www.nominum.com.`

Name Resolution Example

The *nominum.com* name server *ns1.sanjose* responds with *www.nominum.com's* address
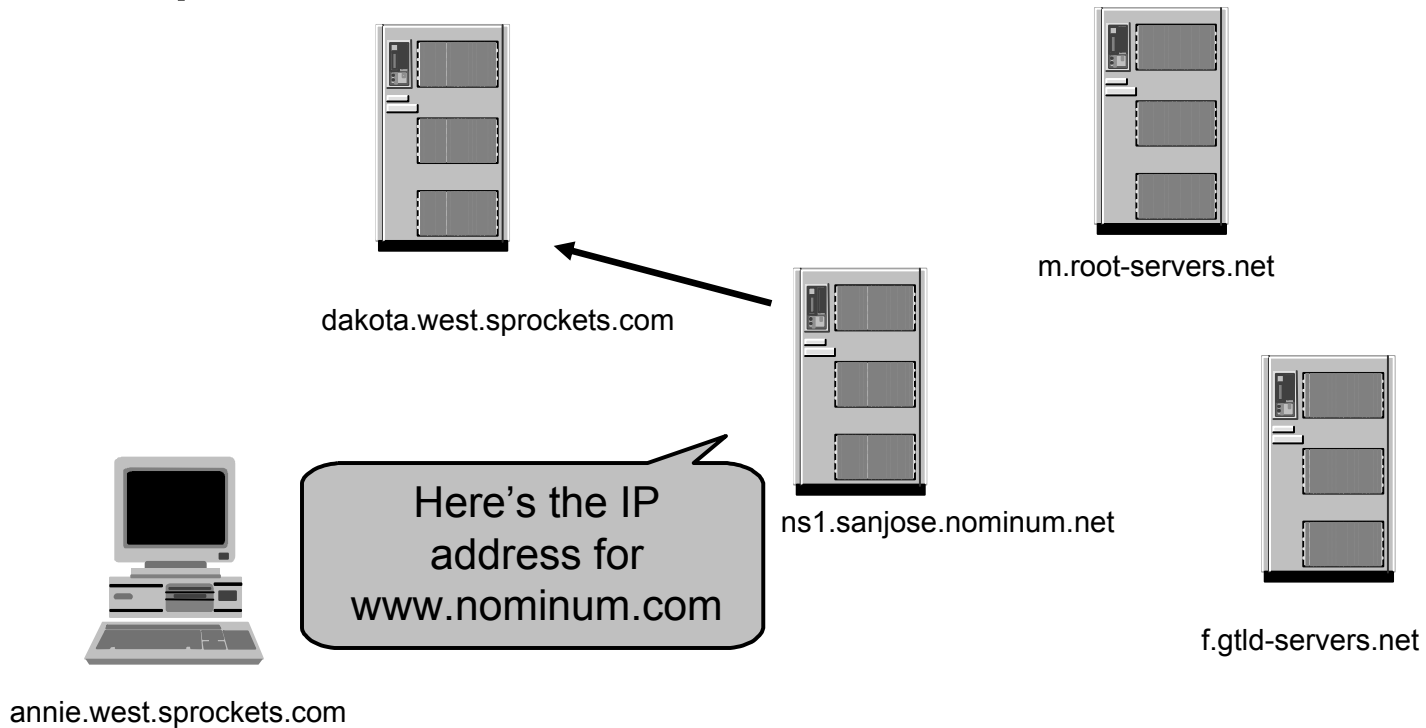
dakota.west.sprockets.com

m.root-servers.net

ns1.sanjose.nominum.net

Here's the IP address for www.nominum.com

f.gtld-servers.net

annie.west.sprockets.com

`ping www.nominum.com.`

Name Resolution Example

The name server *dakota* responds to *annie* with *www.nominum.com's* address

Here's the IP address for www.nominum.com

dakota.west.sprockets.com

m.root-servers.net

ns1.sanjose.nominum.net

f.gtld–servers.net

annie.west.sprockets.com

```
ping www.nominum.com.
```
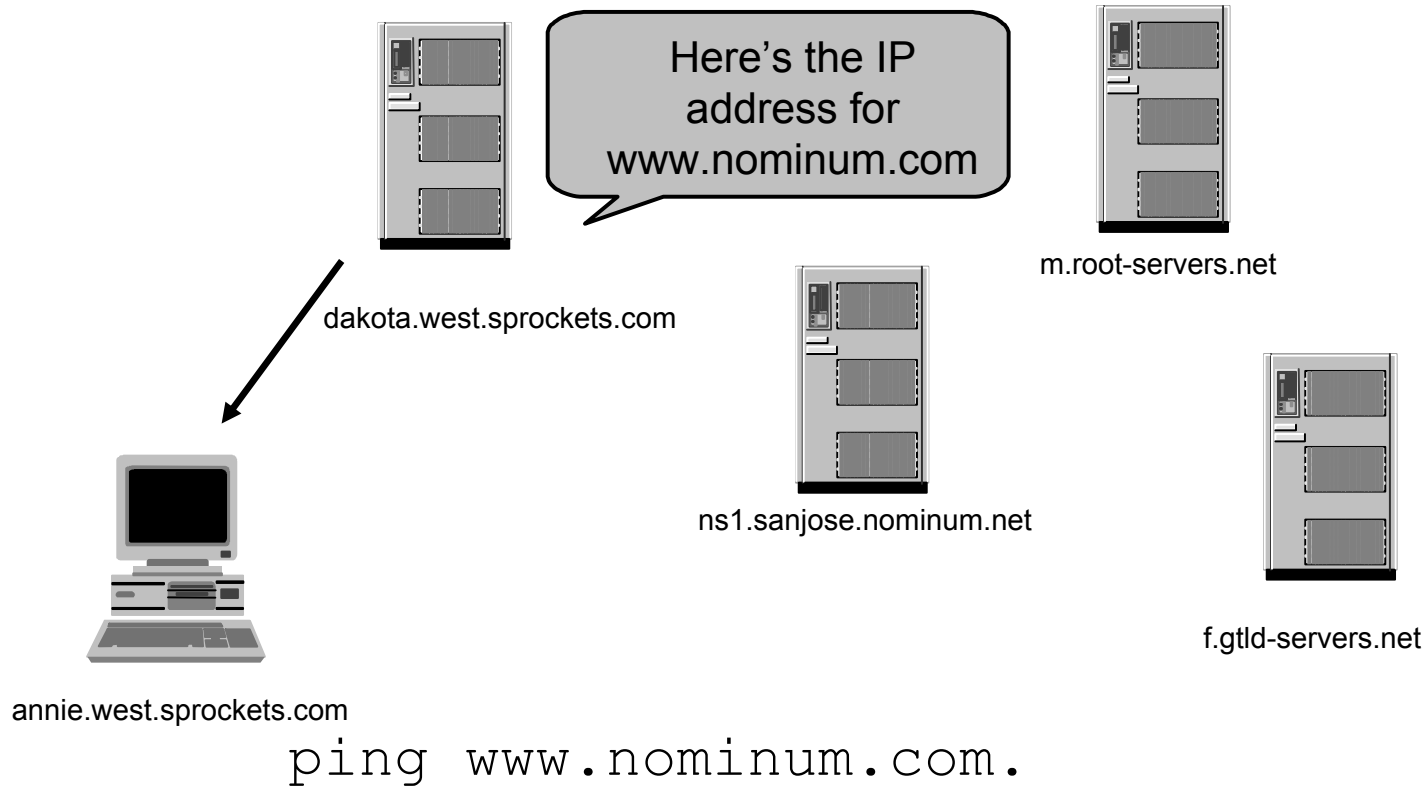
Broad Areas of Concern

- Abruptness
  - No notice or community involvement
  - But internal and private testing
- Is it the right thing?
  - Changes in the core vs innovation
  - Lots more to say
- Competition
  - Not our concern; belongs elsewhere

Initial Advisory

- VeriSign: Please roll back
- Tech Community: Please clarify specs
  - IETF, IAB, network and DNS operators
- ICANN: Please clarify procedures

10/7 Agenda

10:00	Welcome	Arnaud de Borchgrave
		Steve Crocker
10:20	VeriSign Site Finder	
		Scott Hollenbeck
11:00	What was affected	David Shairer
11:30	Community Tech Responses	Paul Vixie
12:00	Information Flow	Richard M. Smith
12:30	LUNCH	
2:00	Protocol Problems and Architectural Issues	Steven M. Bellovin
2:30	Internet Protocols and Innovation	John C. Klensin
3:00	Other Issues; Open Session	
3:30	Next Steps	Steve Crocker
4:00	Adjourn	

10/15 Agenda

Time	Topic	Presenter
1:00	Welcome	Steve Crocker
1:15	VeriSign Business Overview of Site Finder	Anthony Renzette
1:45	Technical Review Panel Summary	Scott Hollenbeck
2:15	Technical Issues and VRSN Responses	Matt Larson
2:45	Usability Market Research	Ben Turner
3:15	Next Steps	Chuck Gomes
		Rusty Lewis
3:30	BREAK	
3:45	Measuring ISP Responses to SiteFinder	Benjamin Edelman
4:15	Global Name Registry Statement	Hakon Haugnes
		Geir Rasmussen
4:30	Other Issues; Open Session	Steve Crocker

Tentative Issues

- Abruptness
- Rightness
- Systemic Stability
- Confidence
- Technical Clarity
- Process Clarity

- Displaced Costs
- Innovation at core vs edge
- Future architecture
- Role of standards
- Existing wild card use
  - .museum, .name, etc

Next Steps

- More Public Input
  - Secsac-comment@icann.org
- Report
- ICANN and others will follow through