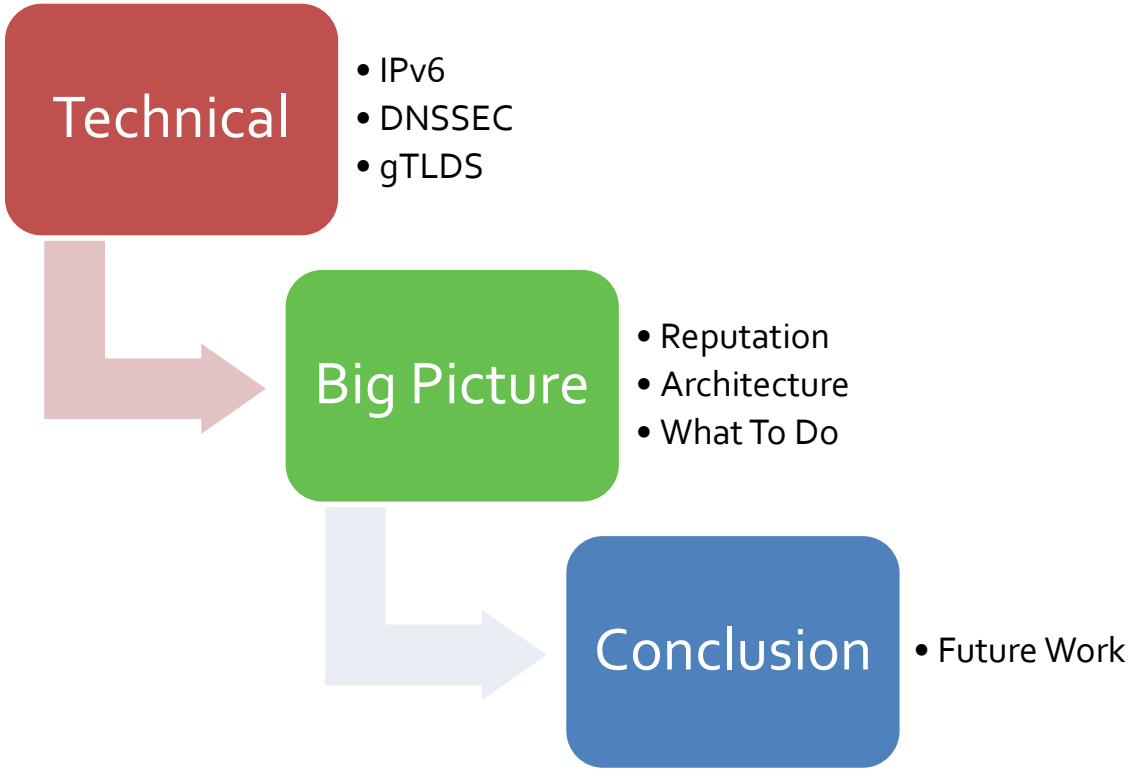
iSECpartners
part of nccgroup

The Myth of Twelve More Bytes

Security on the Post-Scarcity Internet


Technical
• IPv6
• DNSSEC
• gTLDS
Big Picture
• Reputation
• Architecture
• What To Do
Conclusion
• Future Work

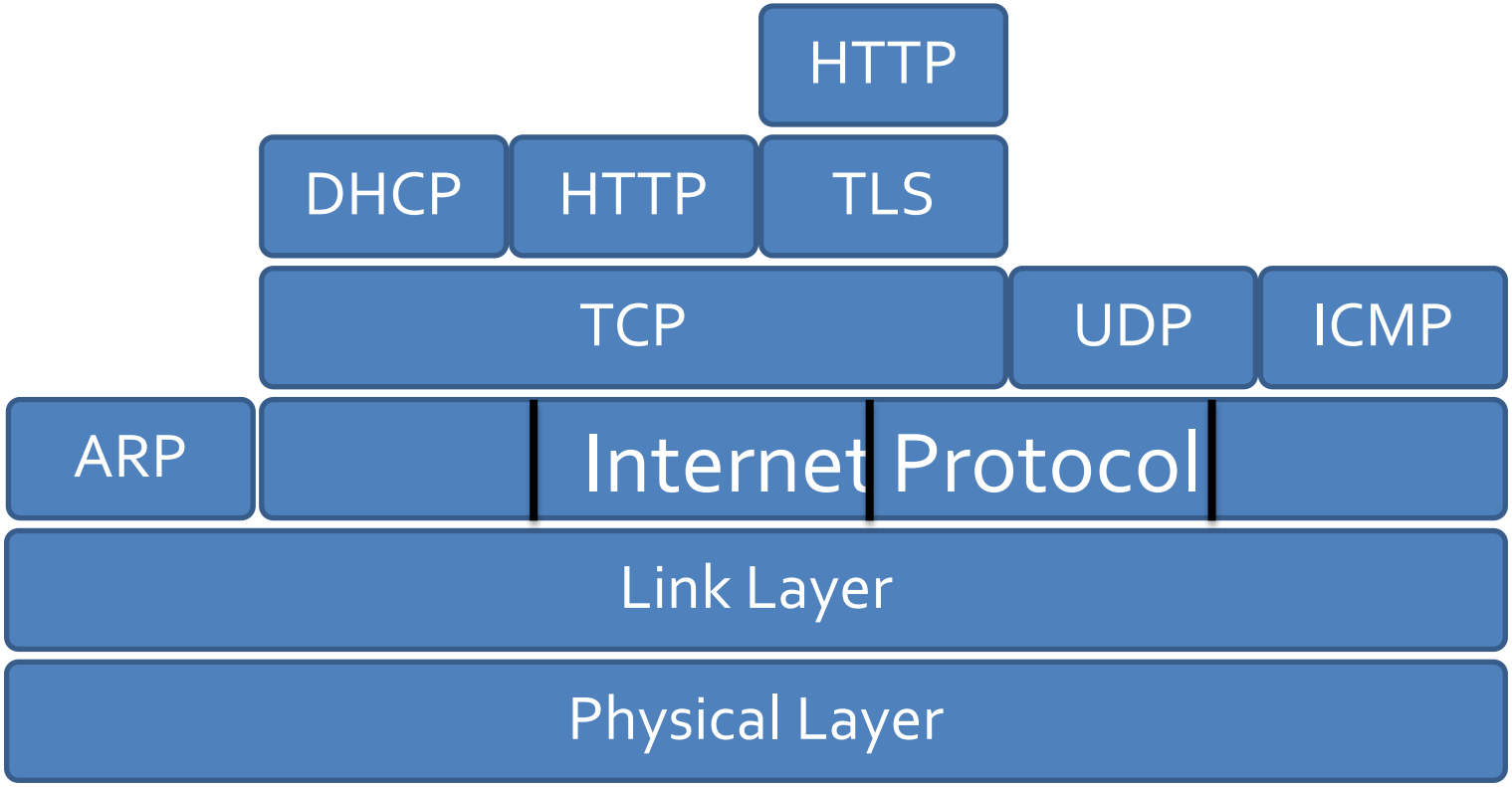
Our Conclusions

iSECpartners part of nccgroup

1. The Internet infrastructure is undergoing fundamental change for the first time in decades
2. The assumption of scarcity is deeply woven into many security assumptions and products
3. The new Internet will face significant problems with trust on both the client and server side
4. New Enterprise Architectures will look very different
5. Everything you have bought will break

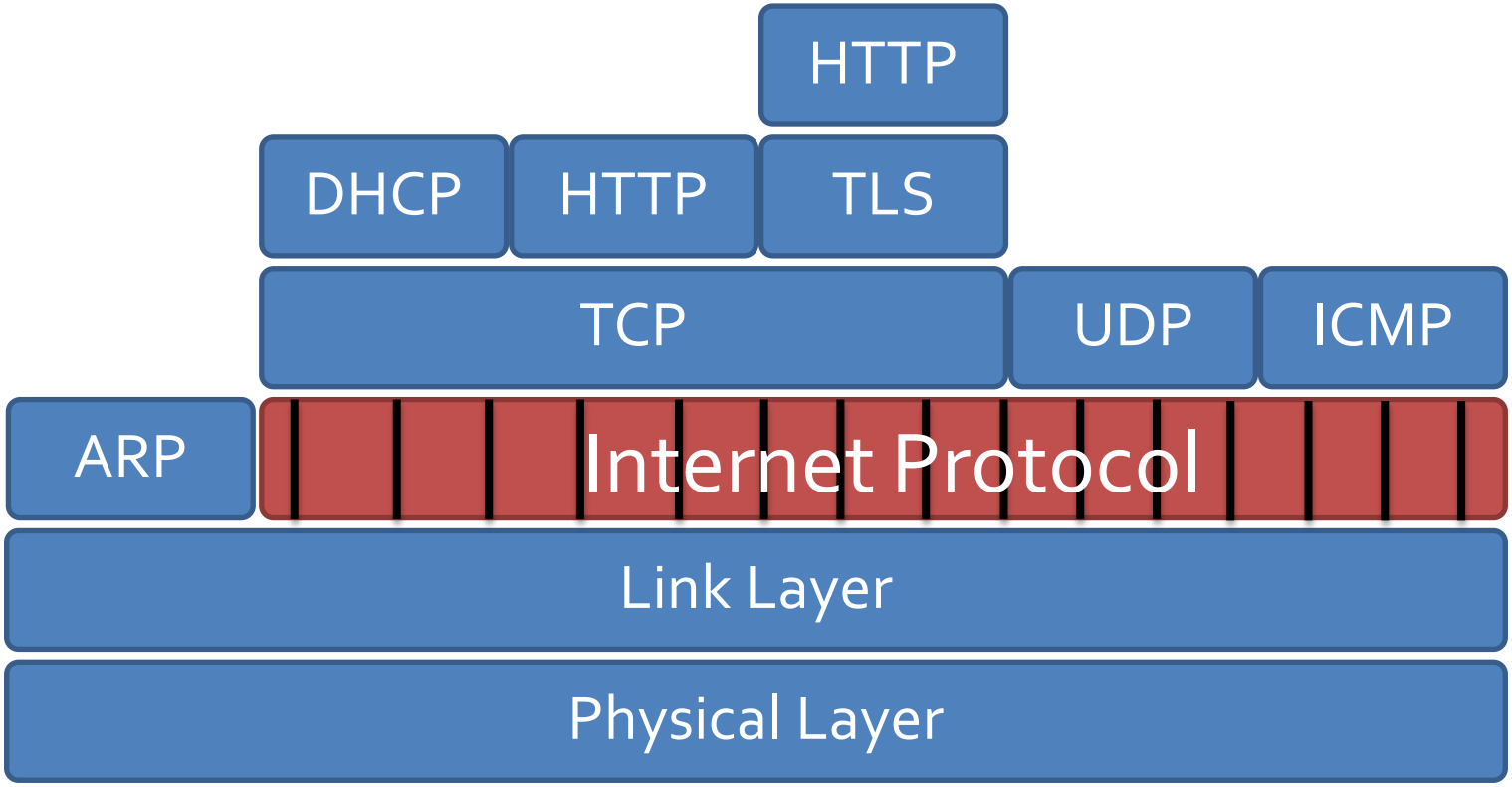
IPv6

iSECpartners part of nccgroup



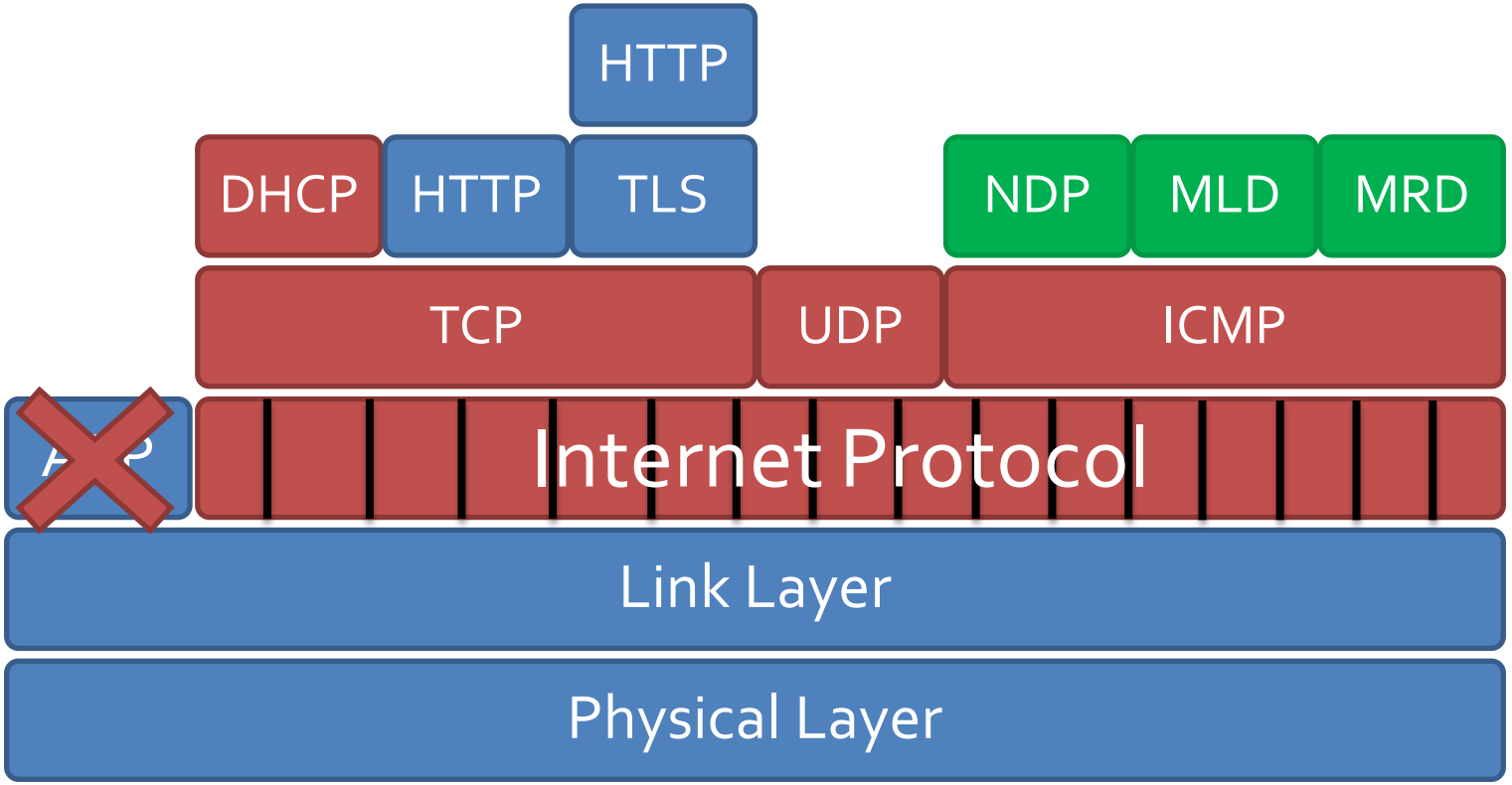
The Myth of 12 More Bytes

iSECpartners part of nccgroup



The Myth of 12 More Bytes

iSECpartners part of nccgroup



iSECpartners
part of nccgroup

Come Join the Party

Stateless Address Auto-Configuration

iSECpartners part of nccgroup

- Give Yourself a local address in your subnet
  - Prefix: fe80:0:0:0: :
  - IPv6 Address: fe80::f03c:91ff:fe96:d927
- Ask what network you're in
  - example: 2600:3c03::
- Take your MAC Address, use it in the prefix
  - MAC: f2:3c:91:96:d9:27
  - IPv6 Address: 2600:3c03::f03c:91ff:fe96:d927

Privacy Addresses

iSECpartners part of nccgroup

- Using your MAC in the last 64 bits identifies you, globally, to every website you visit, no matter where you are
- Super-Mega Evercookie

- RFC 4941 Privacy Addresses
  - Generate a random /64 address
  - Prefer it for outgoing communications

DHCPv6

iSECpartners part of nccgroup

- Conceptually the same as Original DHCP
- Clients can get more than IP Address

The Default For Windows

iSECpartners part of nccgroup

- Windows will happily perform SLAAC
- Windows Prefers IPv6 over IPv4

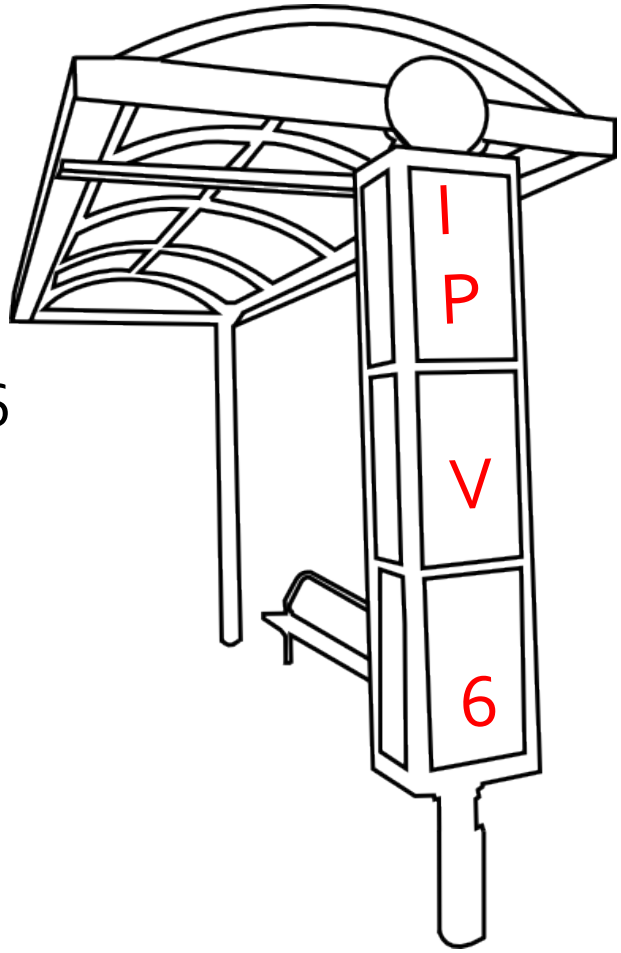
The Default For Windows

iSECpartners part of nccgroup

- Windows will happily perform SLAAC
- Windows Prefers IPv6 over IPv4

Your computers are just sitting around, waiting for someone to help them talk IPv6

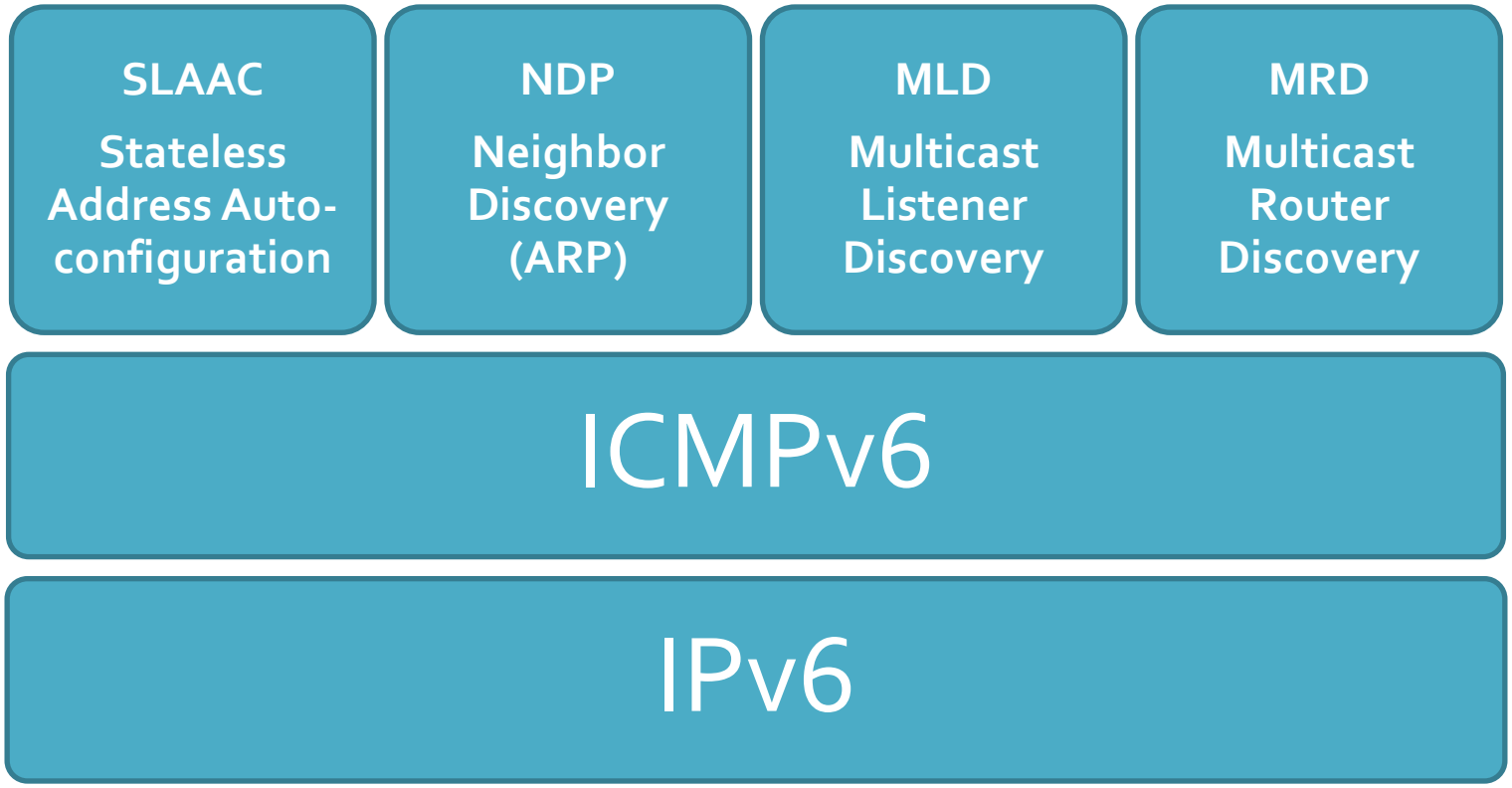
(And it doesn't have to be you.)



iSECpartners
part of nccgroup

ICMPv6

Critical Infrastructure


SLAAC
Stateless Address Auto-configuration
NDP
Neighbor Discovery (ARP)
MLD
Multicast Listener Discovery
MRD
Multicast Router Discovery
ICMPv6
IPv6

ICMPv6 Protocols

iSECpartners part of nccgroup

Router Discovery

iSECpartners
part of nccgroup

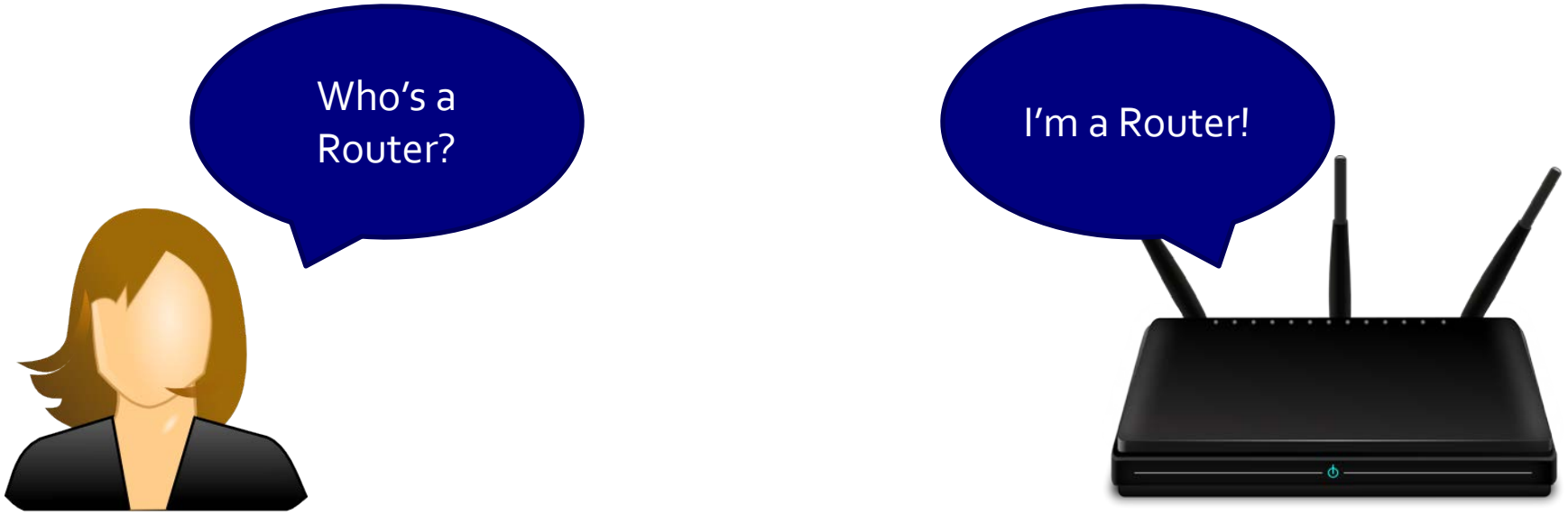
New Protocols
New Protocol Vulnerabilities

(Same Tactics)

NDP

iSECpartners part of nccgroup

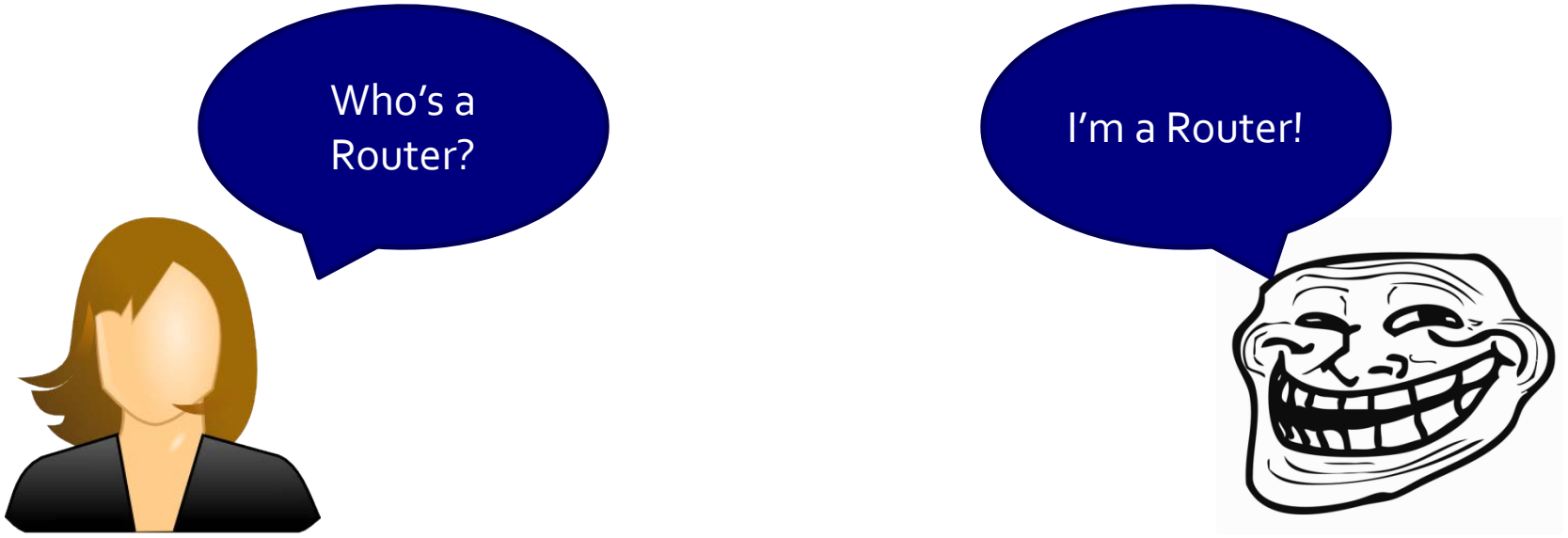
Router Discovery



NDP

iSECpartners part of nccgroup

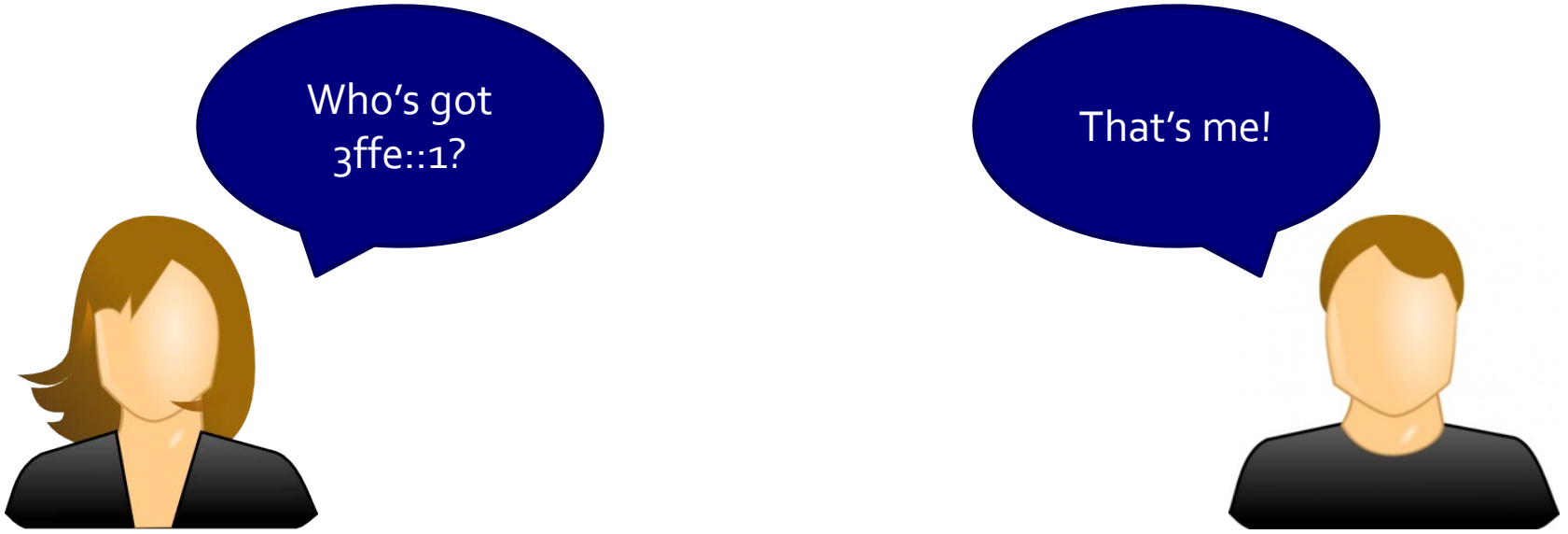
Router Discovery



NDP

iSECpartners part of nccgroup

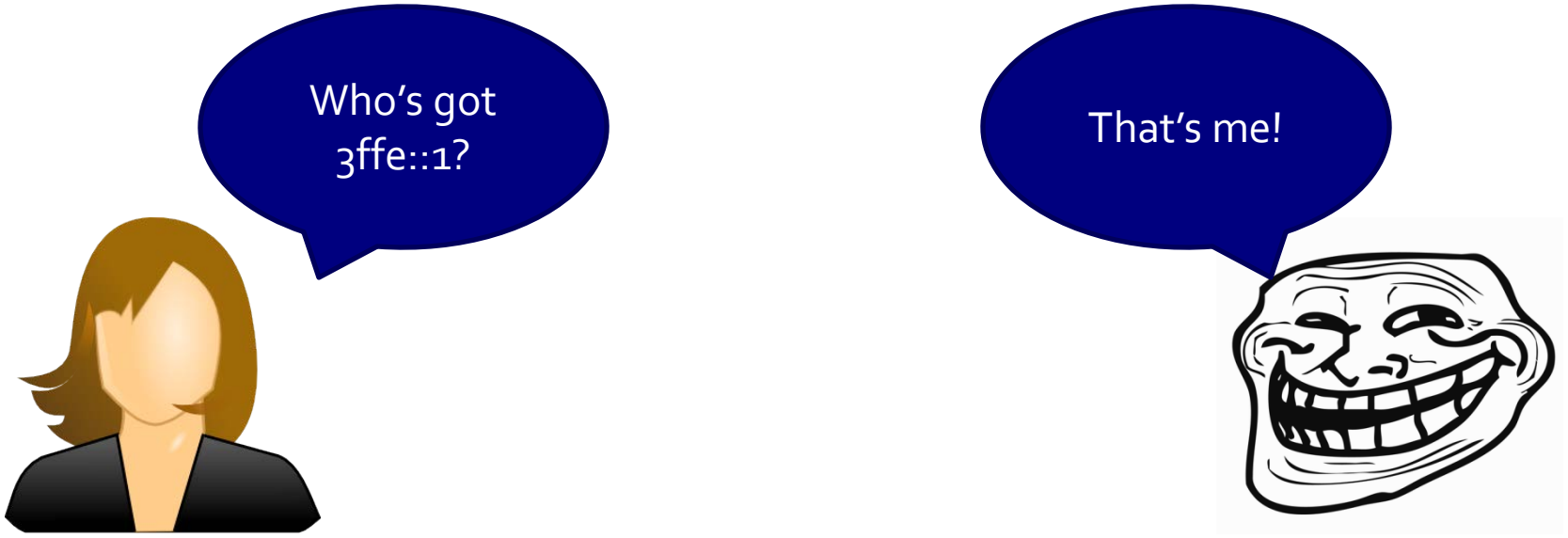
Neighbor Discovery



NDP

iSECpartners part of nccgroup

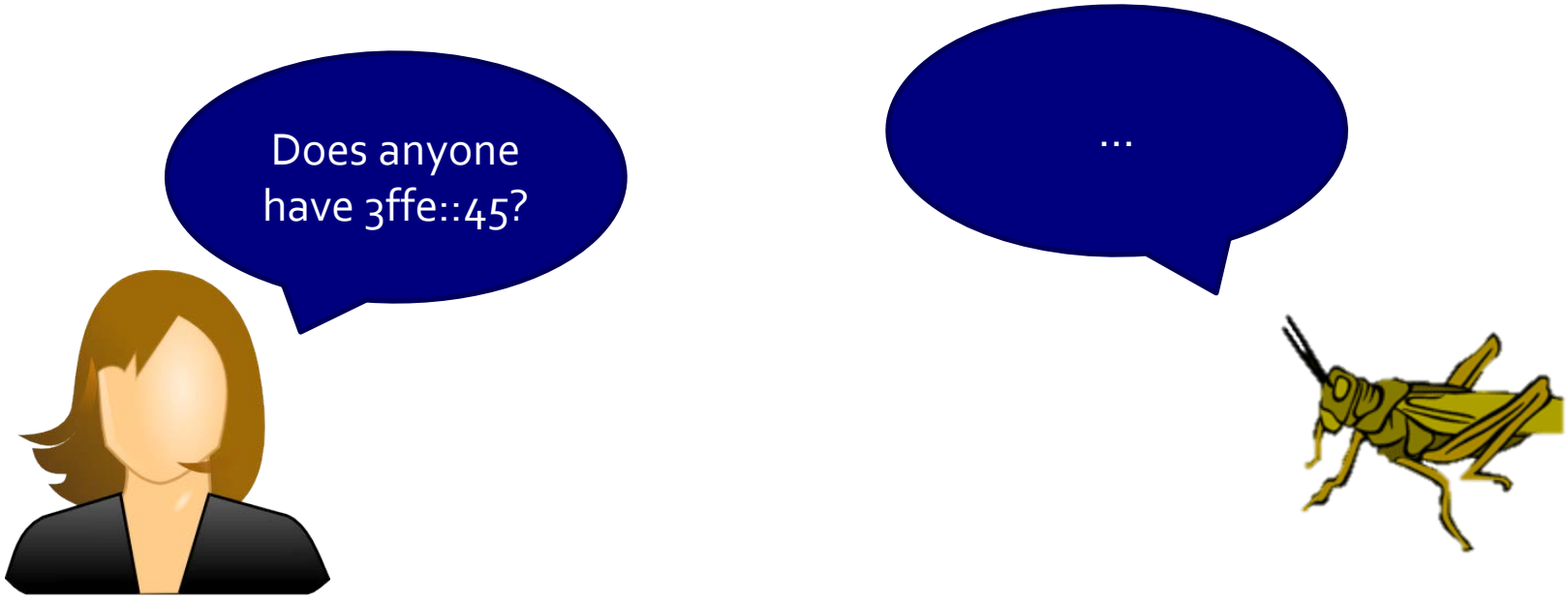
NDP Spoofing is the New ARP Spoofing



ICMPv6 Protocols

iSECpartners part of nccgroup

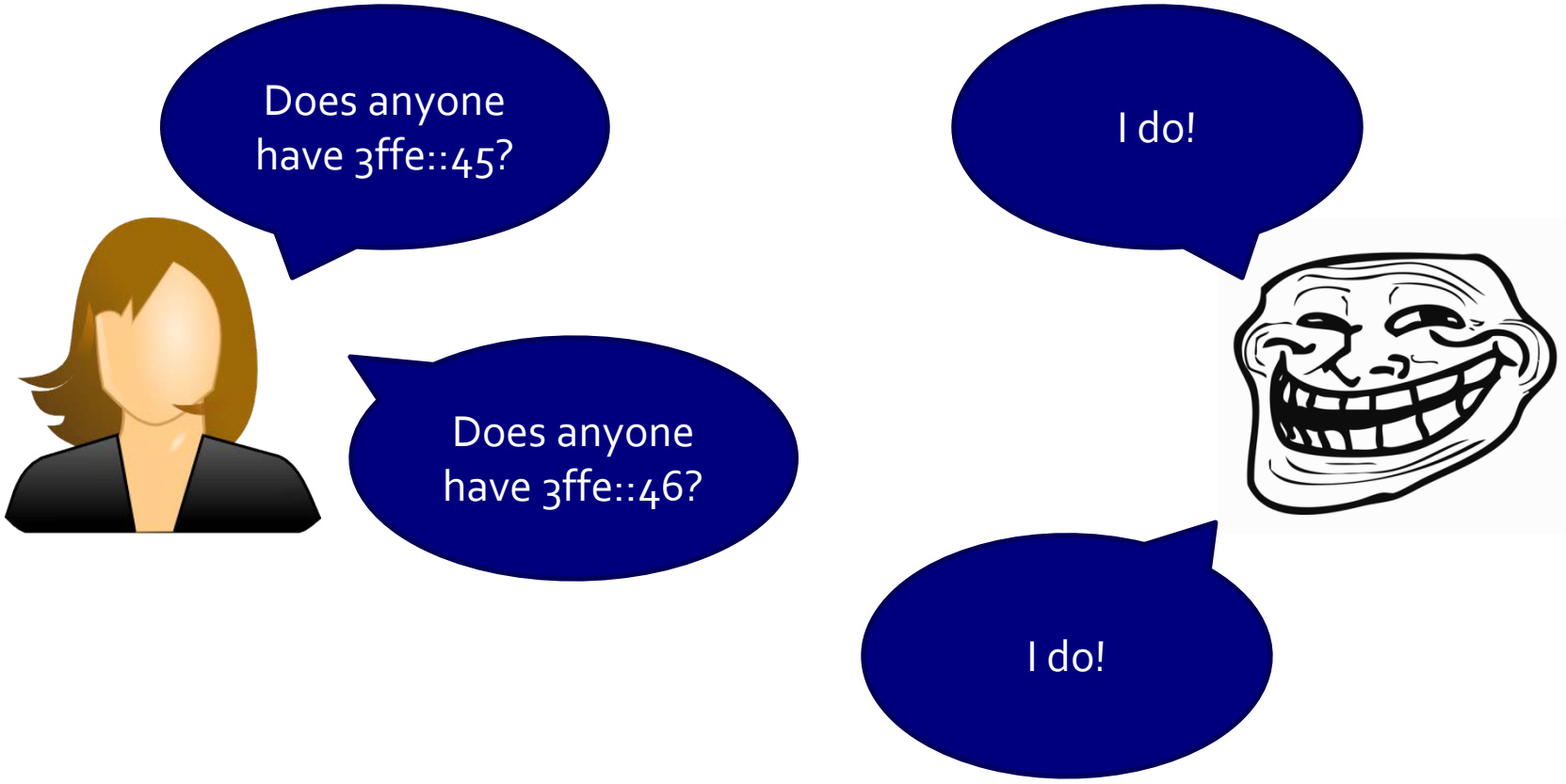
Duplicate Address Detection



ICMPv6 Protocols

iSECpartners part of nccgroup

Duplicate Address Detection



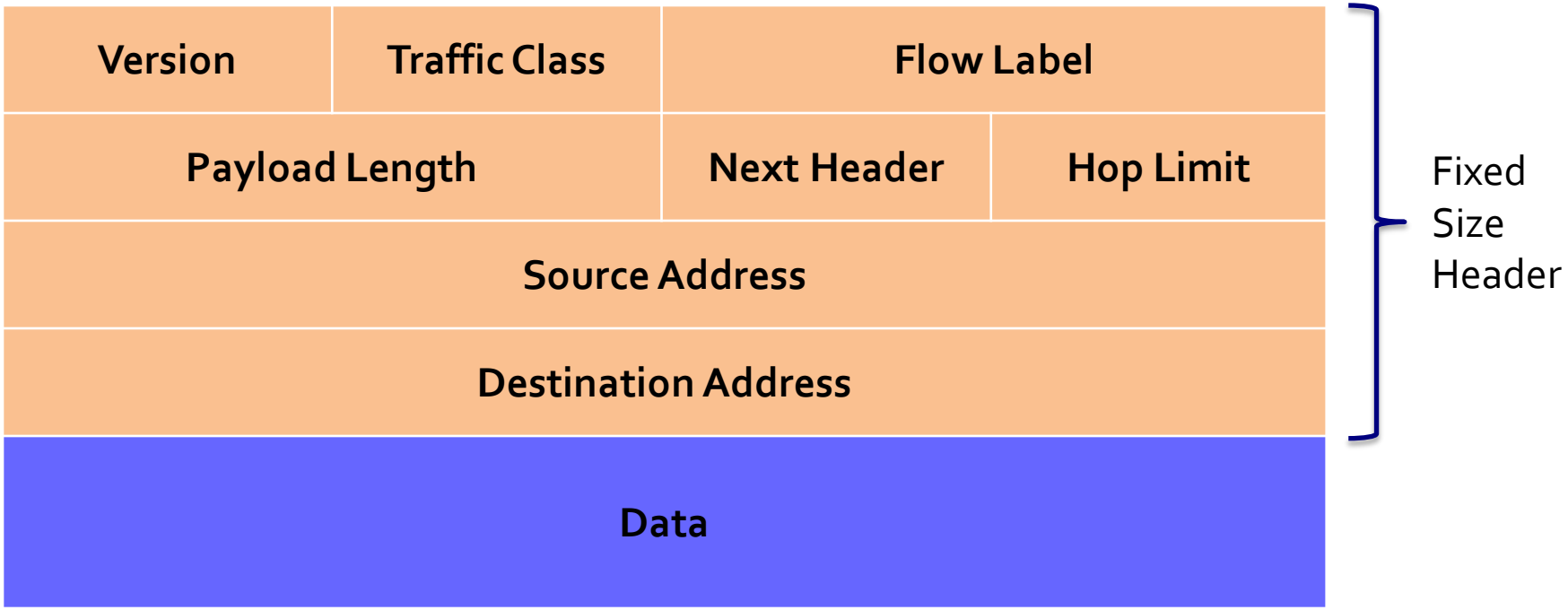
iSECpartners
part of nccgroup

Extension Headers

Pain in the Firewall

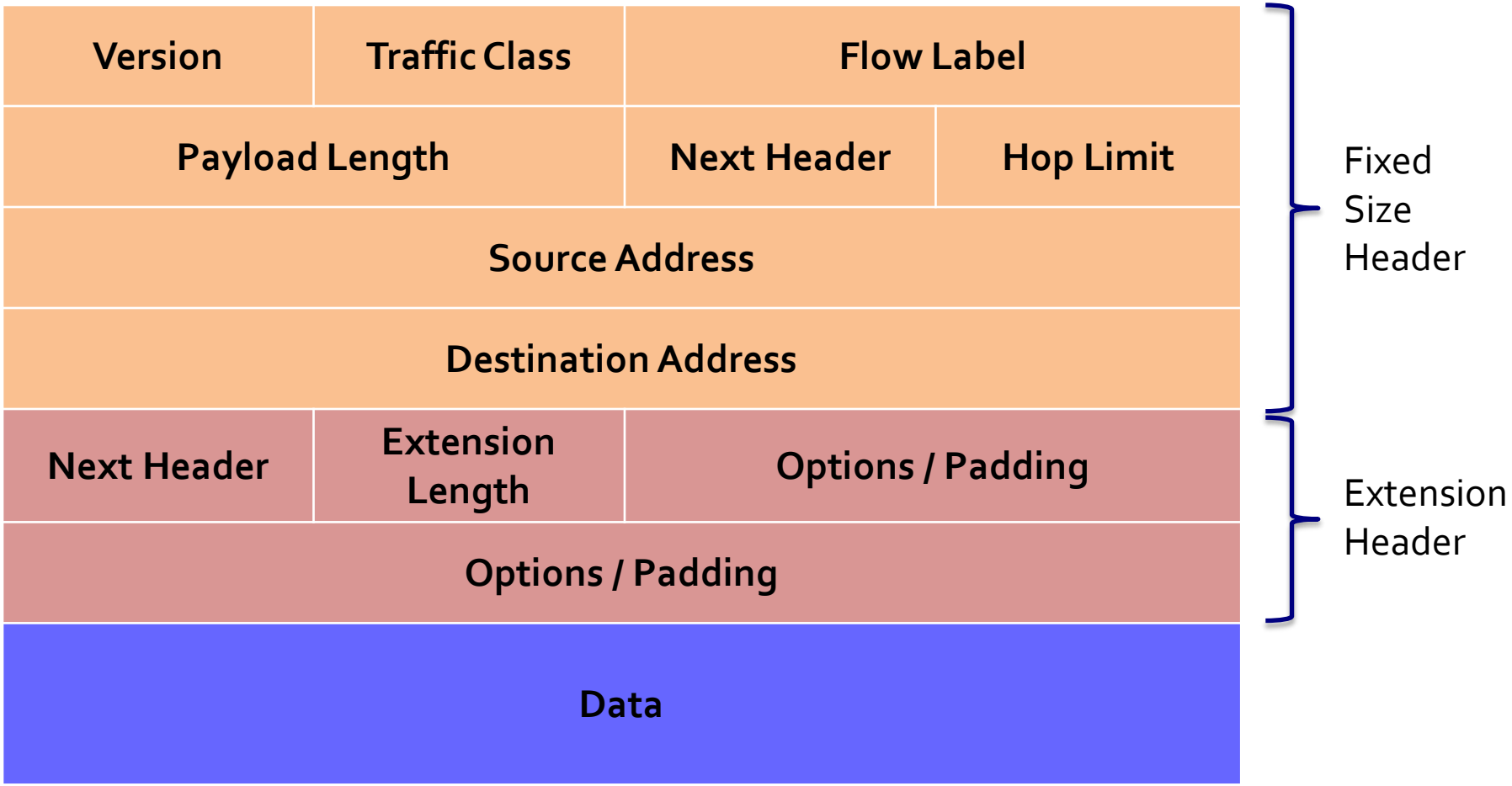
IPv6 Packet Format

iSECpartners part of nccgroup



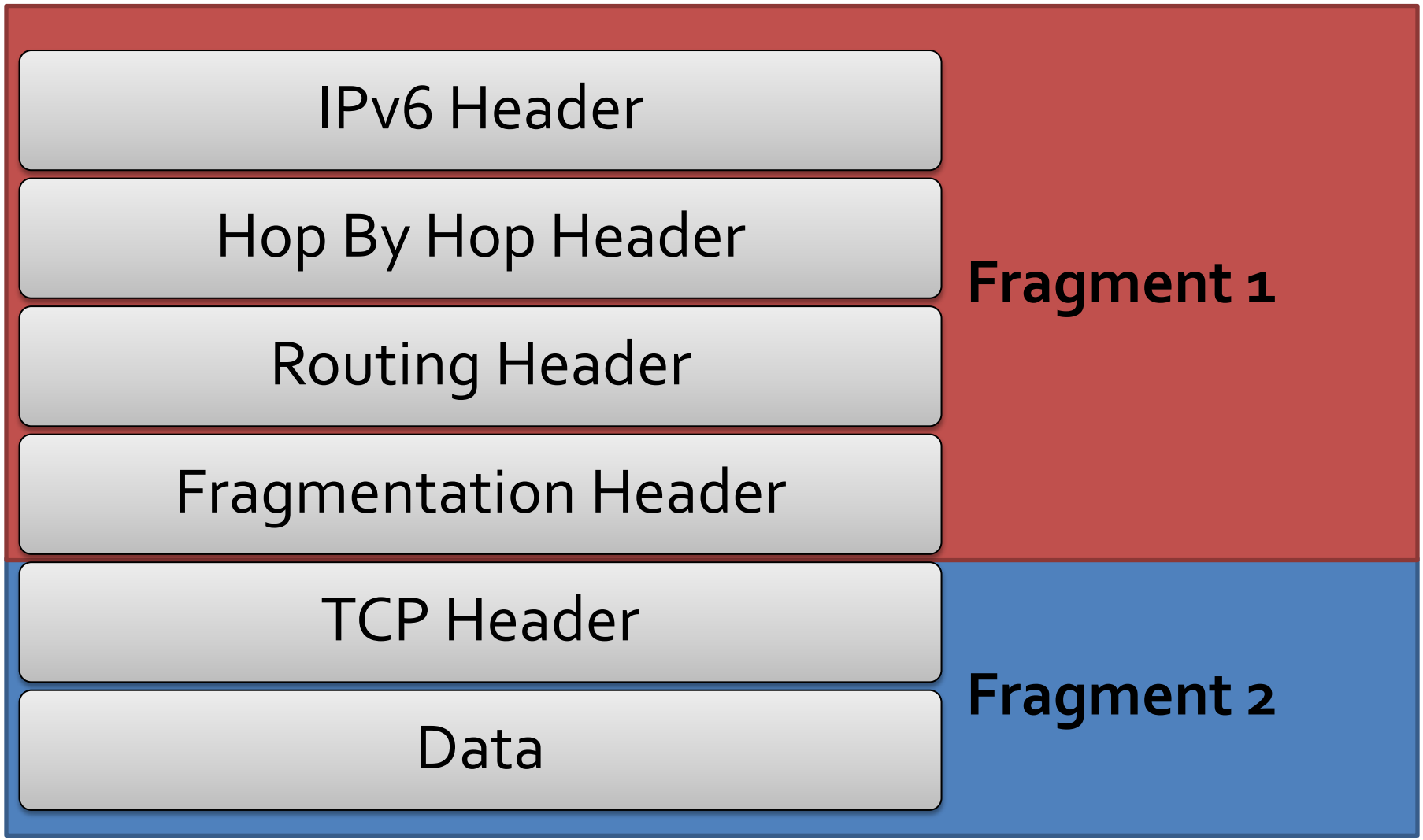
IPv6 Packet Format

iSECpartners part of nccgroup



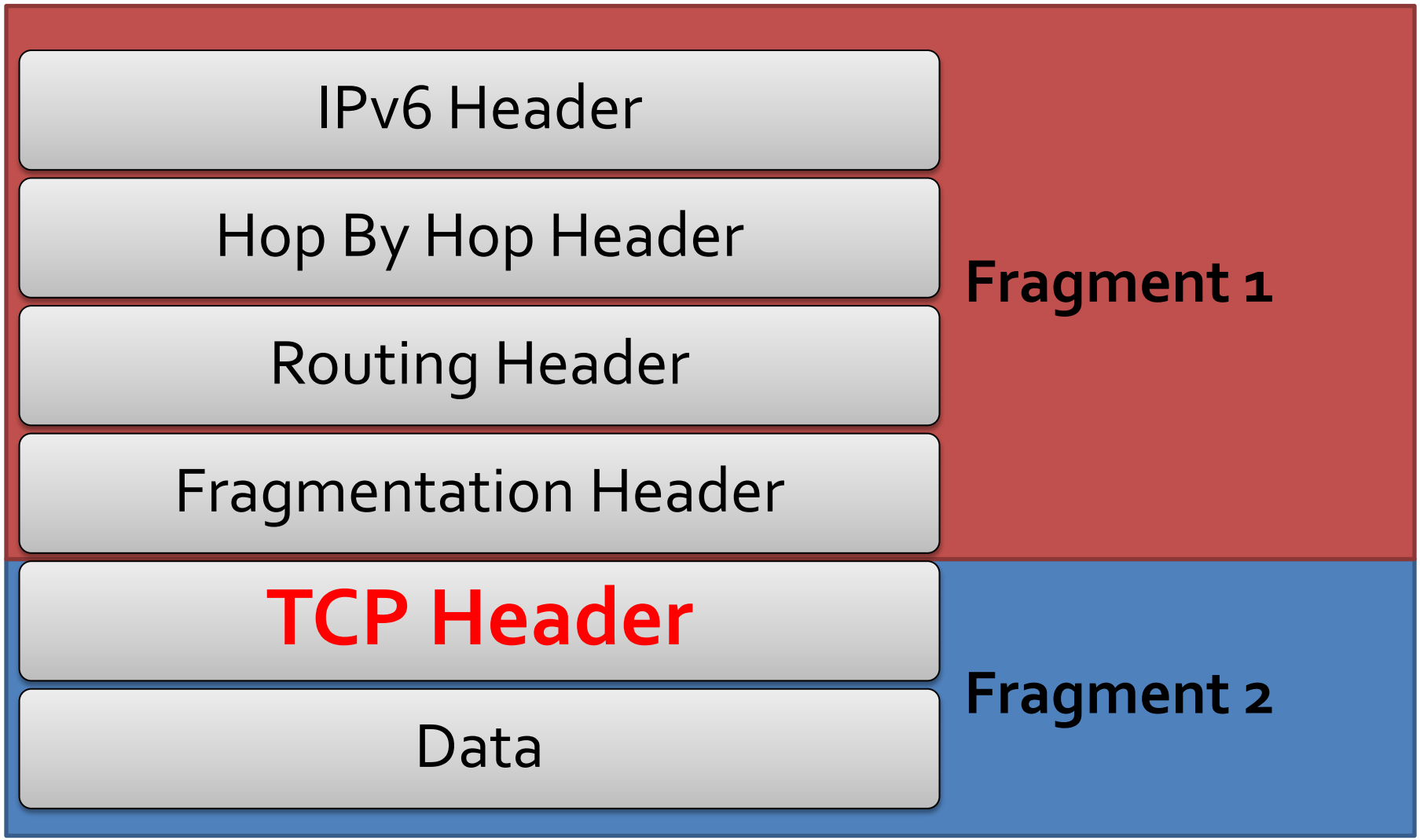
Extension Headers + Fragmentation

iSECpartners part of nccgroup



Stateless Filtering is Impossible

iSECpartners part of nccgroup



iSECpartners
part of nccgroup

Translation & Transition Mechanisms

They're Such Nice Guys.

Translation & Transition

iSECpartners part of nccgroup

Transition

IPv6 Island

|

IPv4 Internet

|

IPv6 Island

Translation

IPv6 < -- > IPv4

Transition

iSECpartners part of nccgroup

6to4

- IPv6 Island to IPv4 Network to IPv6 Island
- Relies on Nice people to run border routers

6rd or IPv6 Rapid Deployment

- 6to4 but instead of nice people, it's an ISP running it, applicable only to their customers

ISATAP

- Host supporting IPv6 sits on an IPv4 Network
- Can talk to IPv6 Internet, but not the reverse

Teredo

- Host supporting IPv6 sits on an IPv4 Network
- Magic NAT-punching IPv6 –in-IPv4 to a Teredo Service Provider (Can be open, can be paid)
- Allows an IPv6 Server to sit in an IPv4 Network

Translation

iSECpartners part of nccgroup

NAT-PT

- Old, Deprecated
- IPv4 or 6 Clients to IPv6 or 4 Servers
- Has External IPv4 addresses for Internal IPv6 Servers
- Breaks a lot of stuff

NAT64

- IPv6 Clients to IPv4 Servers
- Fakes a IPv6 Address for the IPv4 Server
- I talk to the NAT64 device, it forwards to IPv4
- Pairs with DNS64

iSECpartners
part of nccgroup

And More

Time Limits =(

IPv6 Enumeration Mechanisms

iSECpartners part of nccgroup

Internet-Based	
MAC Address Guessing using OUI	24-26 Bits
Sequential Address (DHCPv6 or Sysadmin)	8-16 bits
Reverse Mapping ip6.arpa	Very Efficient
Limited to Local Network	
Multicast Echo nmap	0 Bits
ICMPv6 Parameter Problem nmap	0 Bits
Multicast Listener Discovery nmap	0 Bits
SLAAC Fake-out nmap	0 Bits

Yet More

iSECpartners part of nccgroup

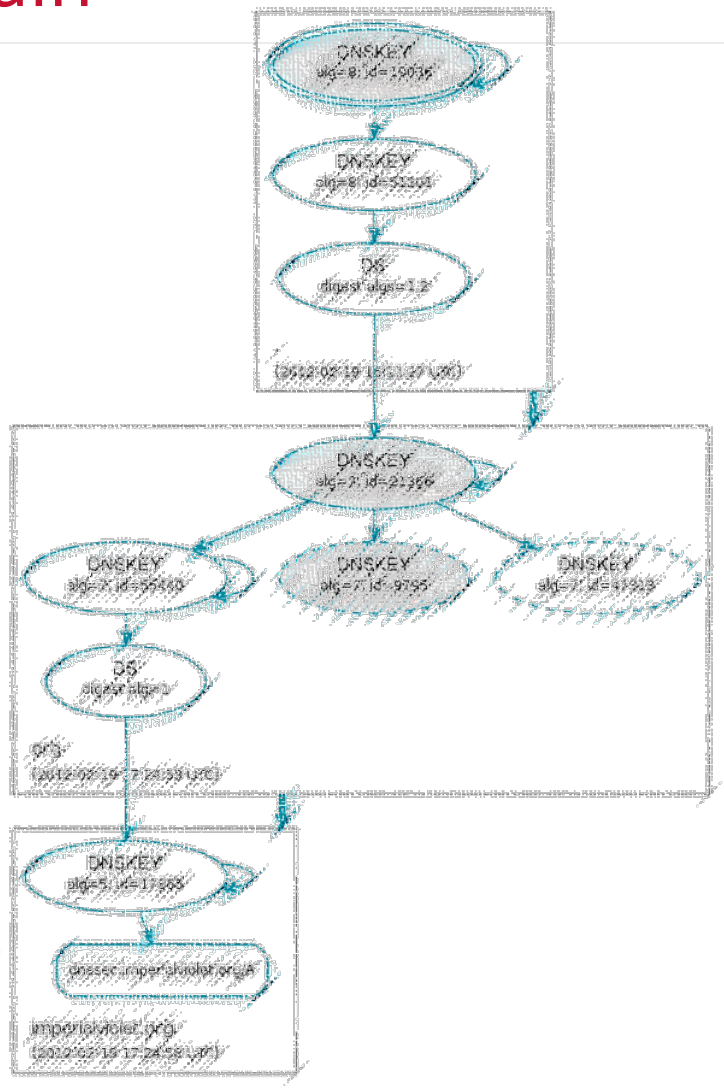
- Multicast!
  - Listener Discovery
  - Listener Enumeration
  - Router Discovery
  - Router Enumeration
- Transition Mechanisms
  - 6to4
  - 6rd
  - 4rd
  - Teredo
  - ISATAP
  - 6in4
  - 6over4
- Node Querying
- UDP/TCP Checksum Calculation
- Router, DHCP, and DNS Discovery
- Redirection
- SeND
- New Features in DHCPv6
- Per-Network Consistent-But-Random Addresses

iSECpartners
part of nccgroup

DNS(SEC)

DNSSEC Chain

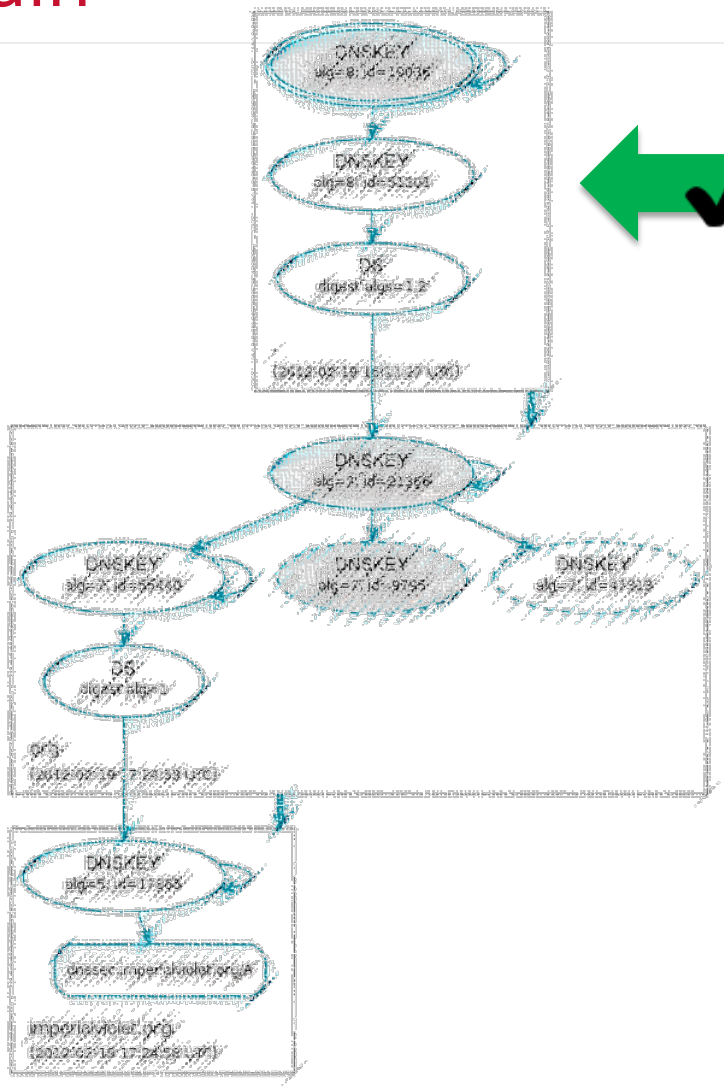
iSECpartners part of nccgroup



att.com ?

DNSSEC Chain

iSECpartners part of nccgroup



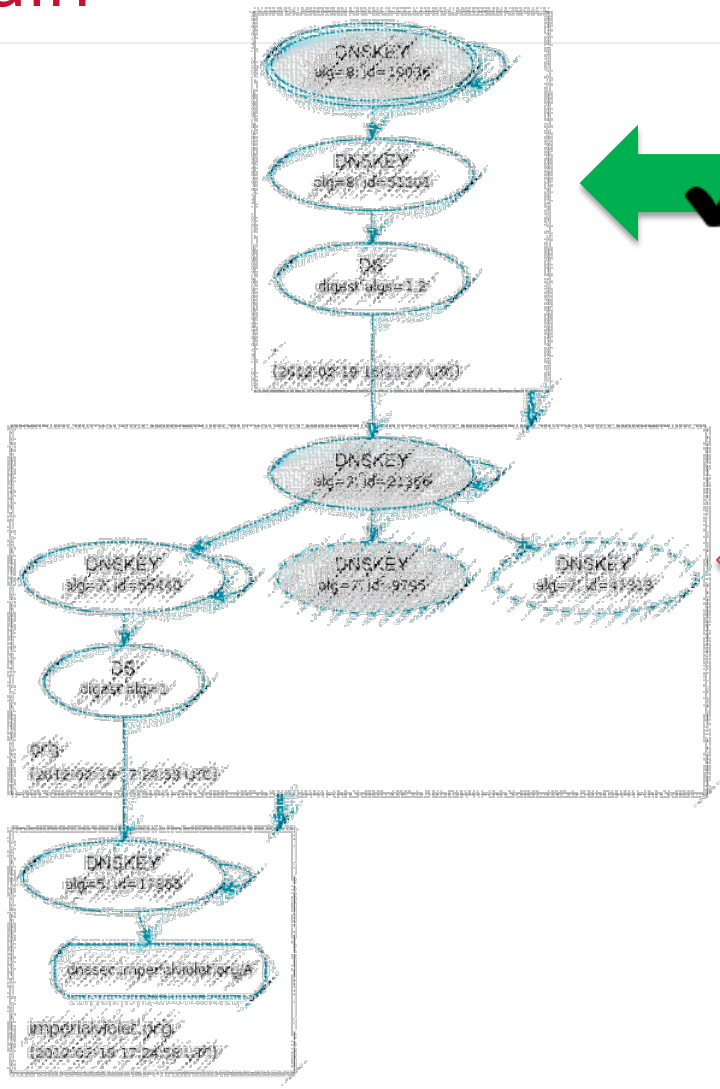
ICANN

att.com

?

DNSSEC Chain

iSECpartners part of nccgroup



ICANN

.com
Verisign

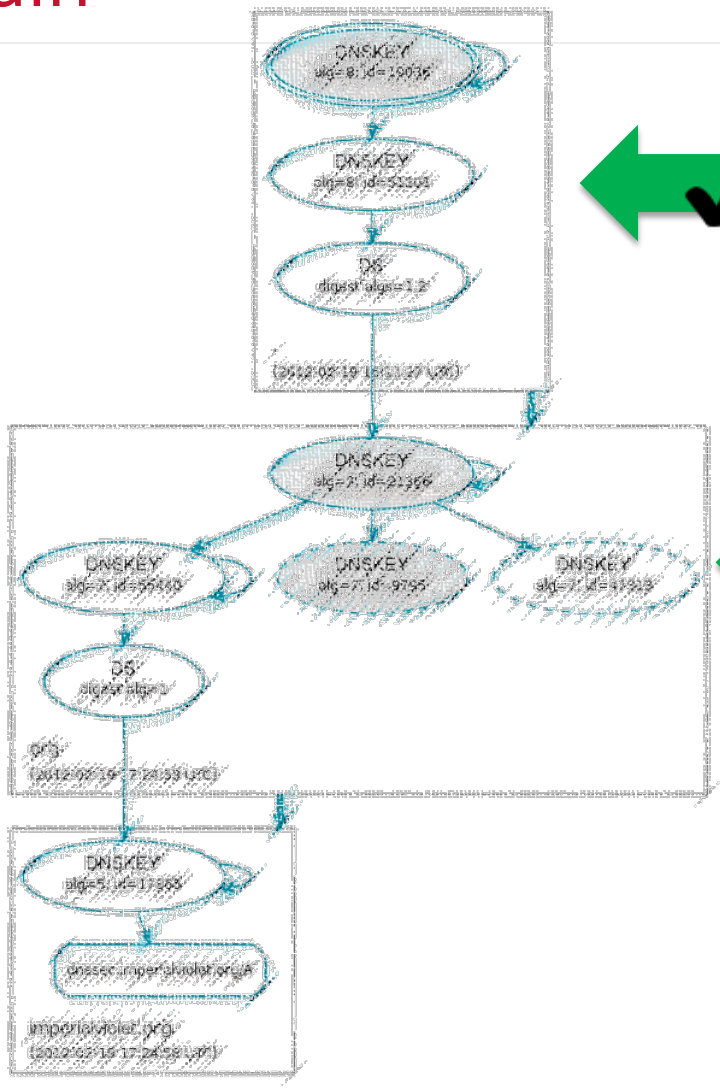
att.com

?

?

DNSSEC Chain

iSECpartners part of nccgroup



ICANN

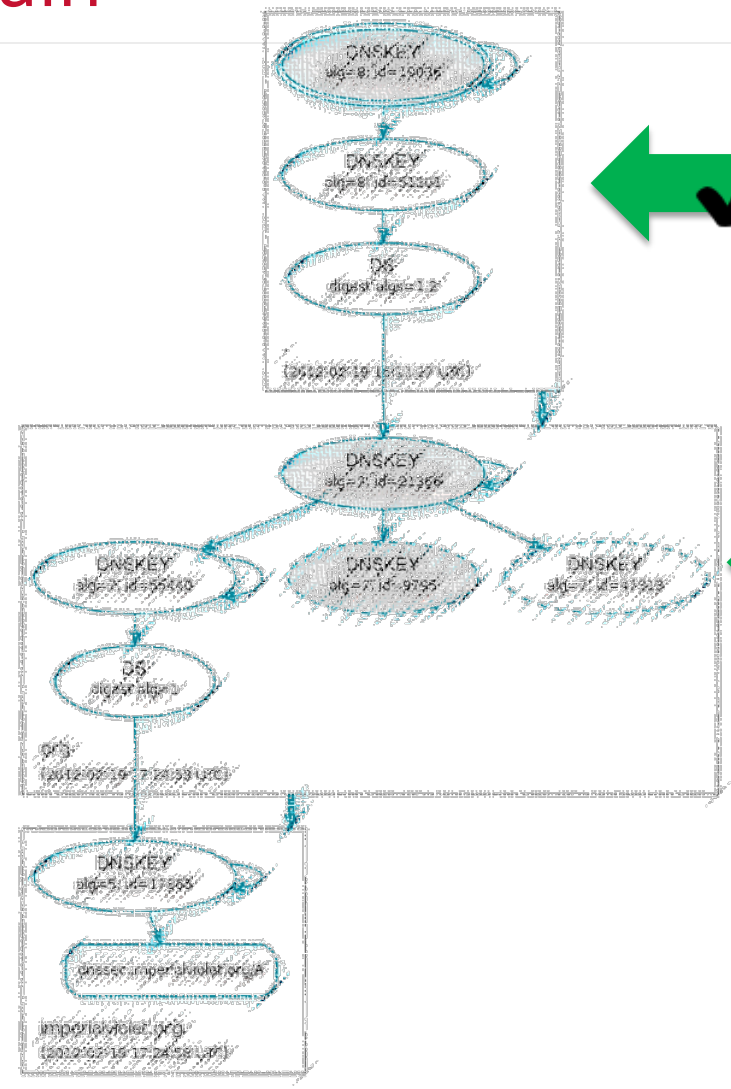
.com
Verisign

att.com

?

DNSSEC Chain

iSECpartners part of nccgroup



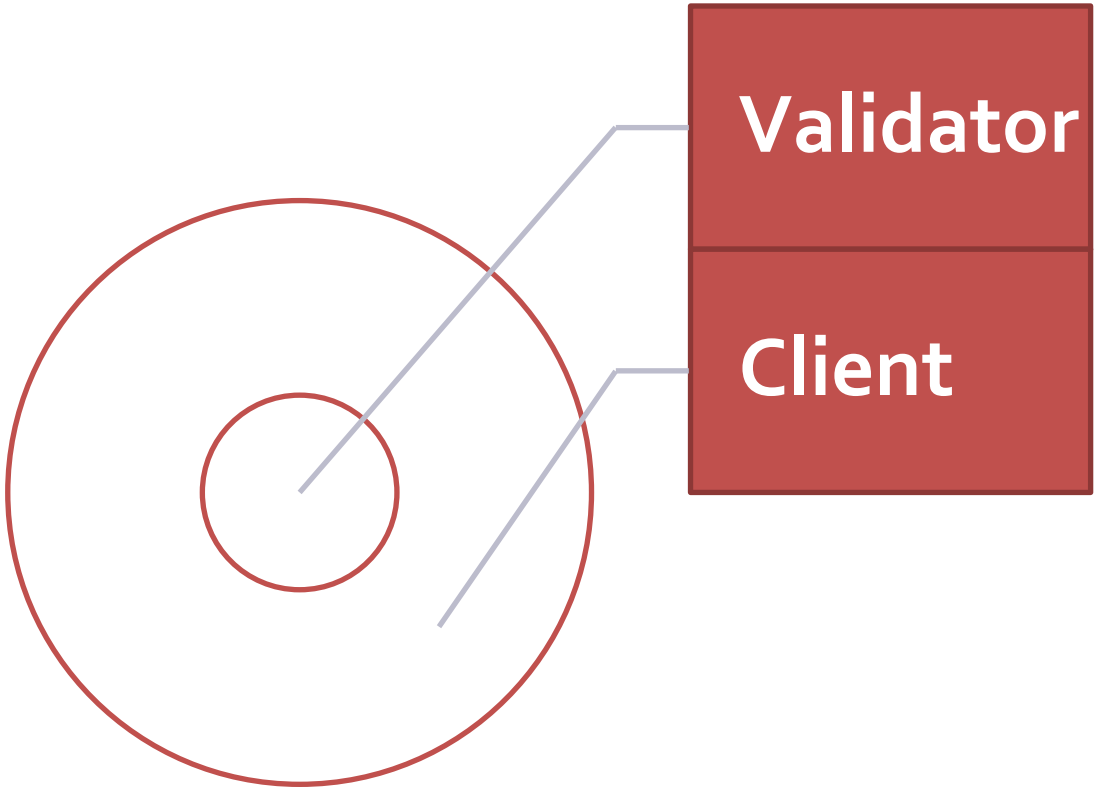
ICANN

.com
Verisign

att.com

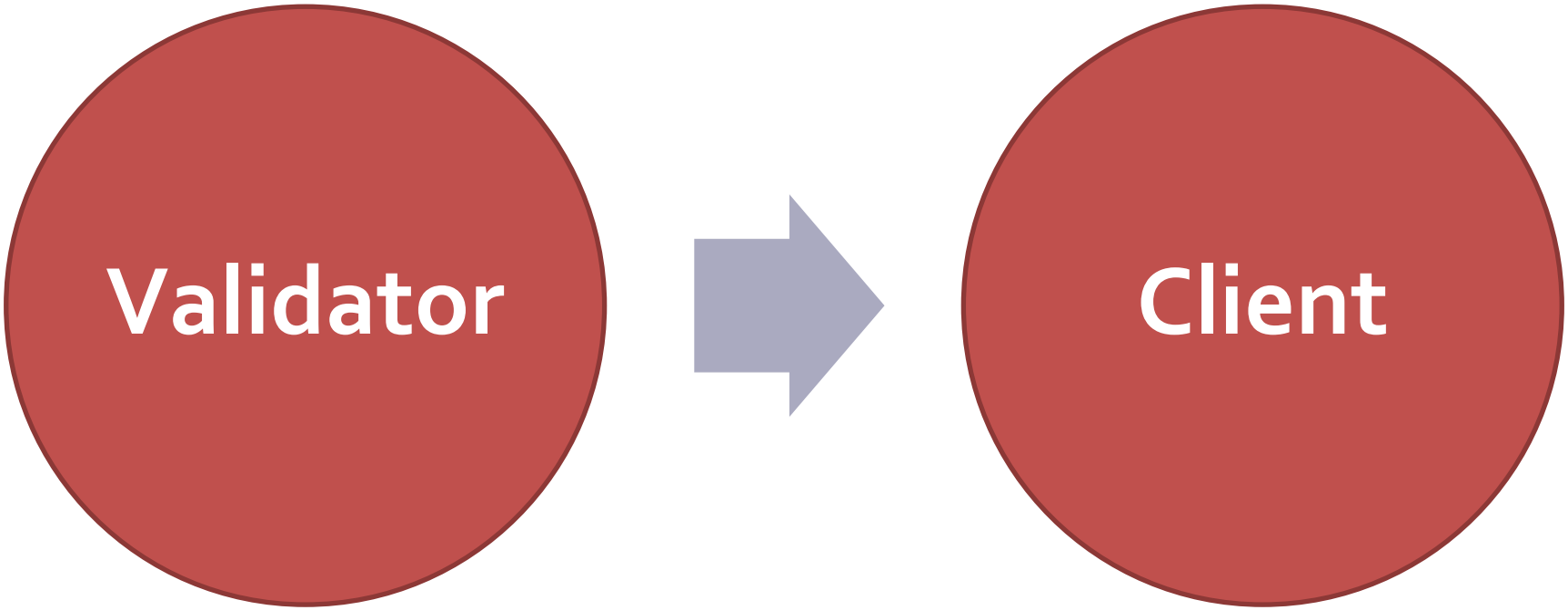
Who verifies the signatures?

iSECpartners part of nccgroup



Who verifies the signatures?

iSECpartners
part of nccgroup



Everything Is Signed

iSECpartners part of nccgroup

```
$ dig +dnssec nic.cz +short
217.31.205.50
A 5 2 1800 20120719160302 20120705160302
40844 nic.cz.
IWGHqGORGO0jh4UuZnwx1P2qoCGYDOcHLhJBIQVJm
h6+0Fskr6Sh2dgj
E6BHQJQJ9HuzSDCHOvJkH98QkK4ZUgMCLSN5DHuVc
mJ/J/g5VMjeWS3i
NmLQVmcvpizwfYVo7cuCg1OteazB2QH7JRp+/KhR+Q
+P8tNpDZKe2kEN VMQ=
```

Everything Is Signed

iSECpartners part of nccgroup

```
$ dig +dnssec nic.cz

;; ANSWER SECTION:

nic.cz.                 1797    IN      A       217.31.205.50

nic.cz.                 1797    IN      RRSIG   A 5 2 1800 20120719160302 20120705160302 40844 nic.cz. IWGHqGORGO0jh4UuZnwx1P2qoCGYDOcHLhJBIQVJmh6+0Fskr6Sh2dgj
E6BHQJQJ9HuzSDCHOvJkH98QkK4ZUgMCLSN5DHuVcmJ/J/g5VMjeWS3i NmLQVmcvpizwfYVo7cuCg1OteazB2QH7JRp+/KhR+Q+P8tNpDZKe2kEN VMQ=


;; AUTHORITY SECTION:

nic.cz.                 1797    IN      NS      a.ns.nic.cz.

nic.cz.                 1797    IN      NS      b.ns.nic.cz.

nic.cz.                 1797    IN      NS      d.ns.nic.cz.

nic.cz.                 1797    IN      RRSIG   NS 5 2 1800 20120719160302 20120705160302 40844 nic.cz. aAWmFODbEaHEt6NxuaIu82wWiL+9jMMH+EvBx4jDS5ViydnSV/lb+hLr
dEZlVgBOSG5VdGKZ2y7cx8fGF8w9/9U1FioVowFfP0dOnZ5ZGAS9dNxm CzHV0+1LiiY0KKSUvPHq9y+thOOwfgkwkFEiofvvRtck1rh8fGfZCFL8 4JY=


;; ADDITIONAL SECTION:

a.ns.nic.cz.            1797    IN      A       194.0.12.1

b.ns.nic.cz.            1797    IN      A       194.0.13.1

d.ns.nic.cz.            1797    IN      A       193.29.206.1

a.ns.nic.cz.            1797    IN      AAAA    2001:678:f::1

b.ns.nic.cz.            1797    IN      AAAA    2001:678:10::1

d.ns.nic.cz.            1797    IN      AAAA    2001:678:1::1

a.ns.nic.cz.            1797    IN      RRSIG   A 5 4 1800 20120719160302 20120705160302 40844 nic.cz. Aj/zemlwTy2FM8+XDZPlDSKhcoKtKSSySugtqrQ8YZx/nOe7i3l/4H3D
XW7cQO/ND1lpW5VR+1RLbsQuovhAcQRtJj47WTkxYwWa4GdWH327aNn2 aklCdCOz6F8bGqZ2Af9EGqIZY+0Rk22FIqZc2qLpNoukI0Hfc0a6OP82 9/E=

b.ns.nic.cz.            1797    IN      RRSIG   A 5 4 1800 20120719160302 20120705160302 40844 nic.cz. XZVf0rEBg1R1j1KHGXt/2lx76s5EbBqfe9a2tU3eyO0MnudsKiPu1VM4
+cBLIgVDUsZMhOaX7i/qHaLAaTa98CucKIQKiwsVVG9kQEWV+OmMrZE3 01xjVd6KNGq77jDyEVz2l6yiTIt/8U7KHDtM3haUXITeyUGJZcJvZ3Ta IOc=

d.ns.nic.cz.            1797    IN      RRSIG   A 5 4 1800 20120719160302 20120705160302 40844 nic.cz. nFN5NWMibodVQYurwwdOlLIQbEWR0hSH+6OJDGRnsCpGGXiWr9VdeAhM
XFWehN/uVa6a+TpwJgnJFYkPzDVrVaFxTGdgNqqTFNcVtwLupbvc6Qq0 Nh6/0yKxbFEkK7n4R0m9Akwnr0BXVkdkpwy3xvZZGlMvfJMq/AKESqlD t3A=

a.ns.nic.cz.            1797    IN      RRSIG   AAAA 5 4 1800 20120719160302 20120705160302 40844 nic.cz. ghUpNuAs+8F08OfPucZg3/P+dOqQRdTYHoZVH8toyEcFqSTU3+yIp7HB
+O9hStK2RASMLi8lonzASZ2YbQRPZXmoBN+zEAZi6s3PIf3EFx7V388A UMowRyTyeh1qvf7fHn0llHDc2K1L4TZ5ZFuUg2PVNBaqcSSdI1mLDHsX AUM=

b.ns.nic.cz.            1797    IN      RRSIG   AAAA 5 4 1800 20120719160302 20120705160302 40844 nic.cz. MxlTDSe0Dkfyzbf9qdDj0Cs0oWrMpzkRsN8g4mfi1uWMuYlHTdUuu9d/
ec27we65x5B/SJJ6+Lb40A030BuuzJyvpuPNvpXh1fFCLZuvNuFPbhs9 MbptJmuEKjutraaA8jnxgK1KLT4kB+Nekf2IrwSC3oxAoyn5wXZJF0Fu /6o=

d.ns.nic.cz.            1797    IN      RRSIG   AAAA 5 4 1800 20120719160302 20120705160302 40844 nic.cz. AIRg88oIb4AR1QYeu5J0VBd6pjgeHI8vWAvJzy7m7O6Mmpn+KldrHu4M
gz7vOYPWZK8qNSvE/lDm7GZ3vERbVvprCwsvzaZCTb8h2wo1VxPx9tVA GQLo2yPTtX9gUqNBMRr/xS7CwyJLVNy3ZJTrQ3G8HyYOyRUVf/SubxPr srI=
```

Signatures Are Large

iSECpartners part of nccgroup

Protocol	Length	Info
DNS	77	Standard query A nic.cz
DNS	259	Standard query response A 217.31.205.50 RRSIG
DNS	[illegible]	Standard query DNSKEY nic.cz
DNS	1115	Standard query response DNSKEY DNSKEY DNSKEY RRSIG RRSIG

- DNS UDP Limit is 512
- EDNS UDP Limit is 4096
- DNS TCP has no limit

- 24 Residential and SOHO routers were tested
- 18 of 24 Devices tested couldn't support EDNS
- 23 of 24 Devices tested couldn't support TCP
  - http://www.icann.org/en/groups/ssac/documents/sac-053-en.pdf

Everything Is Signed - Including No's

iSECpartners part of nccgroup

Where is doesntexist.att.com?

There is no doesntexist.att.com

RRSIG("There is no doesntexist.att.com", $ATT\text{-}Key_{ZSK}$)

Denial of Service

iSECpartners part of nccgroup

Where is doesntexist1.att.com?

There is no doesntexist1.att.com

RRSIG("There is no doesntexist1.att…", $ATT\text{-}Key_{ZSK}$)

Where is doesntexist2.att.com?

There is no doesntexist2.att.com

RRSIG("There is no doesntexist2.att…", $ATT\text{-}Key_{ZSK}$)

Where is doesntexist3.att.com?

There is no doesntexist3.att.com

RRSIG("There is no doesntexist3.att…", $ATT\text{-}Key_{ZSK}$)

Sign a Single Response?

iSECpartners part of nccgroup

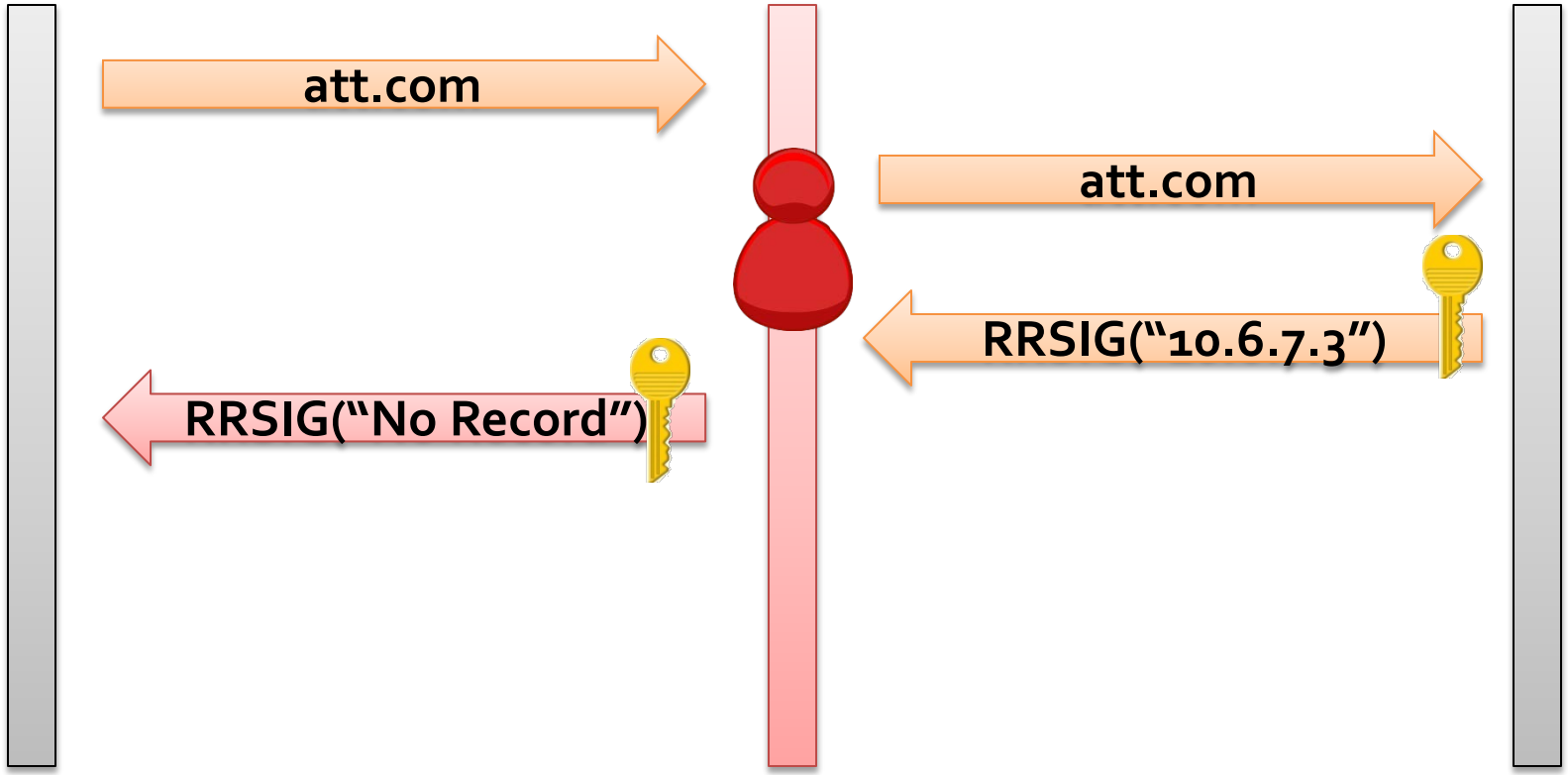
Where is doesntexist.att.com?

No Record

RRSIG("No Record", $ATT\text{-}Key_{ZSK}$)

Man in the Middle

iSECpartners part of nccgroup



Sign The Ranges

iSECpartners part of nccgroup

Where is doesntexist.att.com?

There is nothing between admin.att.com and keyserver.att.com

RRSIG("There is nothing between…", $ATT\text{-}Key_{ZSK}$)

Called NSEC

Information Disclosure

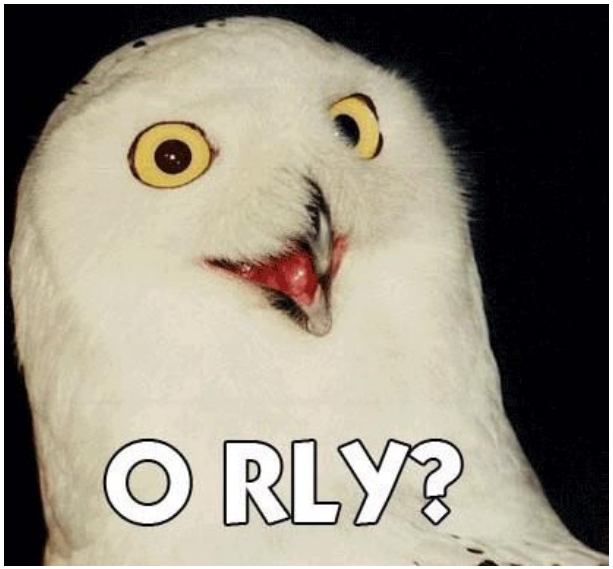
iSECpartners part of nccgroup

Where is doesntexist.att.com?

There is nothing between admin.att.com and

keyserver.att.com

RRSIG("There is nothing between…", $ATT\text{-}Key_{ZSK}$)



Hash, then Sign The Ranges

iSECpartners part of nccgroup

Where is doesntexist.att.com?

doesntexist.att.com -> hash it -> da739562…..

There is nothing between a847629…. and ff572645….

RRSIG("There is nothing between…", $ATT\text{-}Key_{ZSK}$)

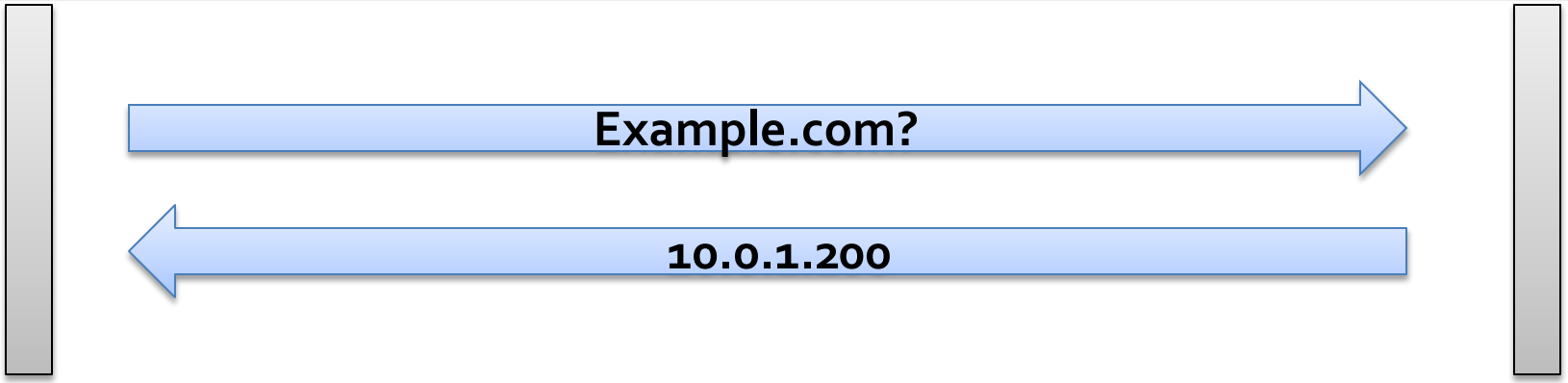
Called NSEC3!

iSECpartners
part of nccgroup

‘Put It In DNSSEC’

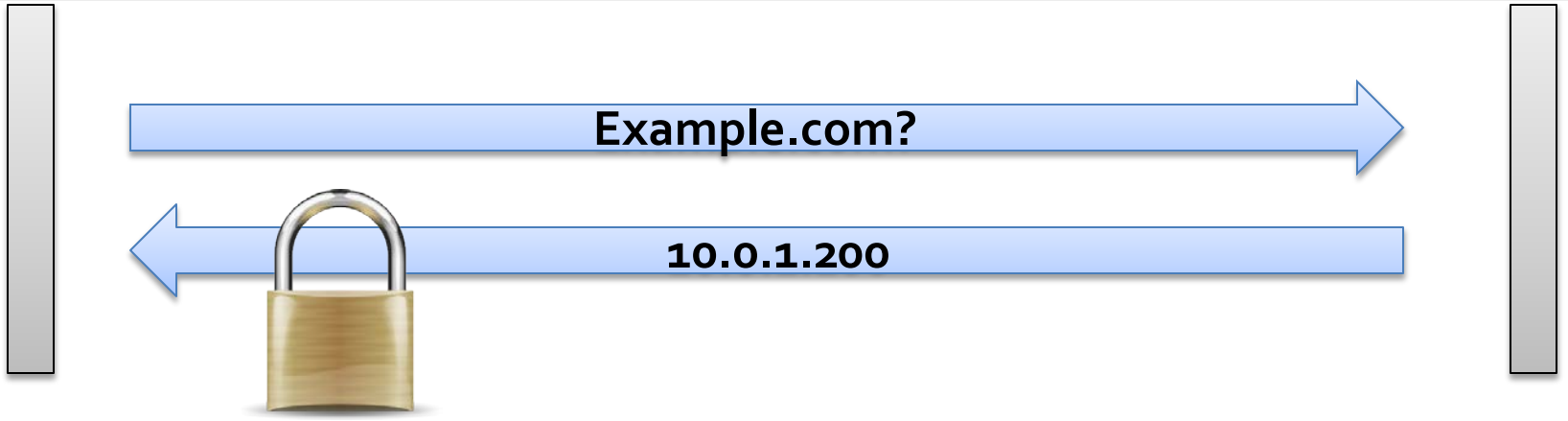
Shoving Stuff in DNSSEC

iSECpartners part of nccgroup



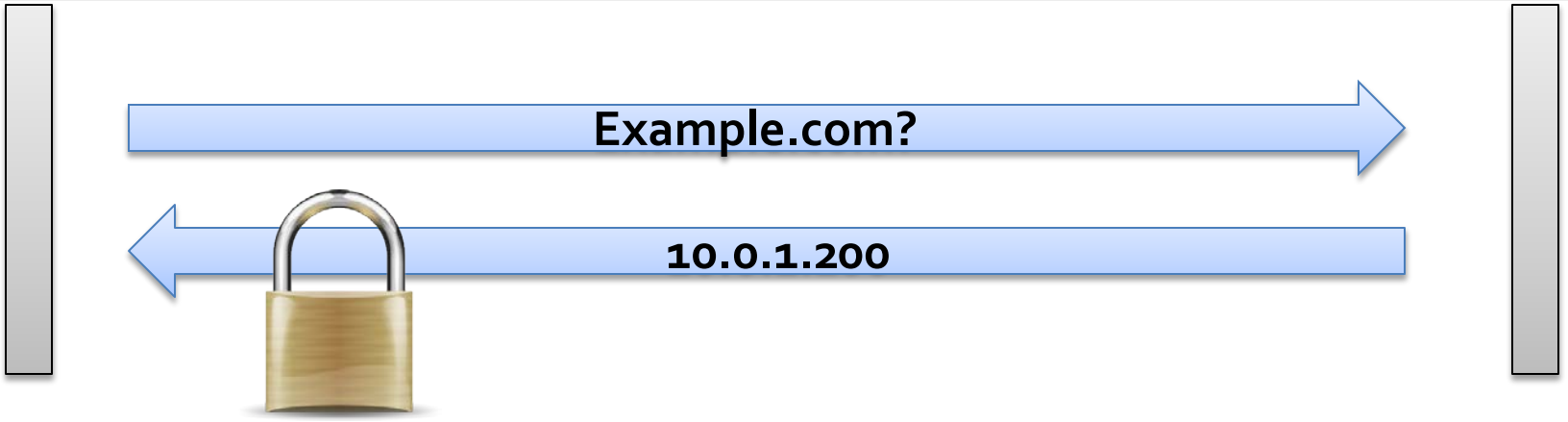
Shoving Stuff in DNSSEC

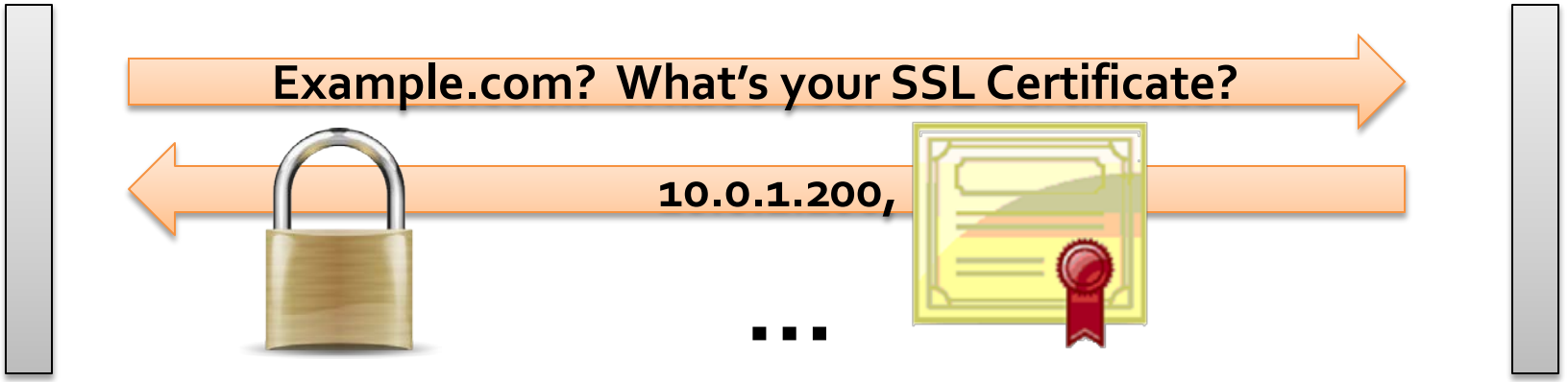
iSECpartners part of nccgroup



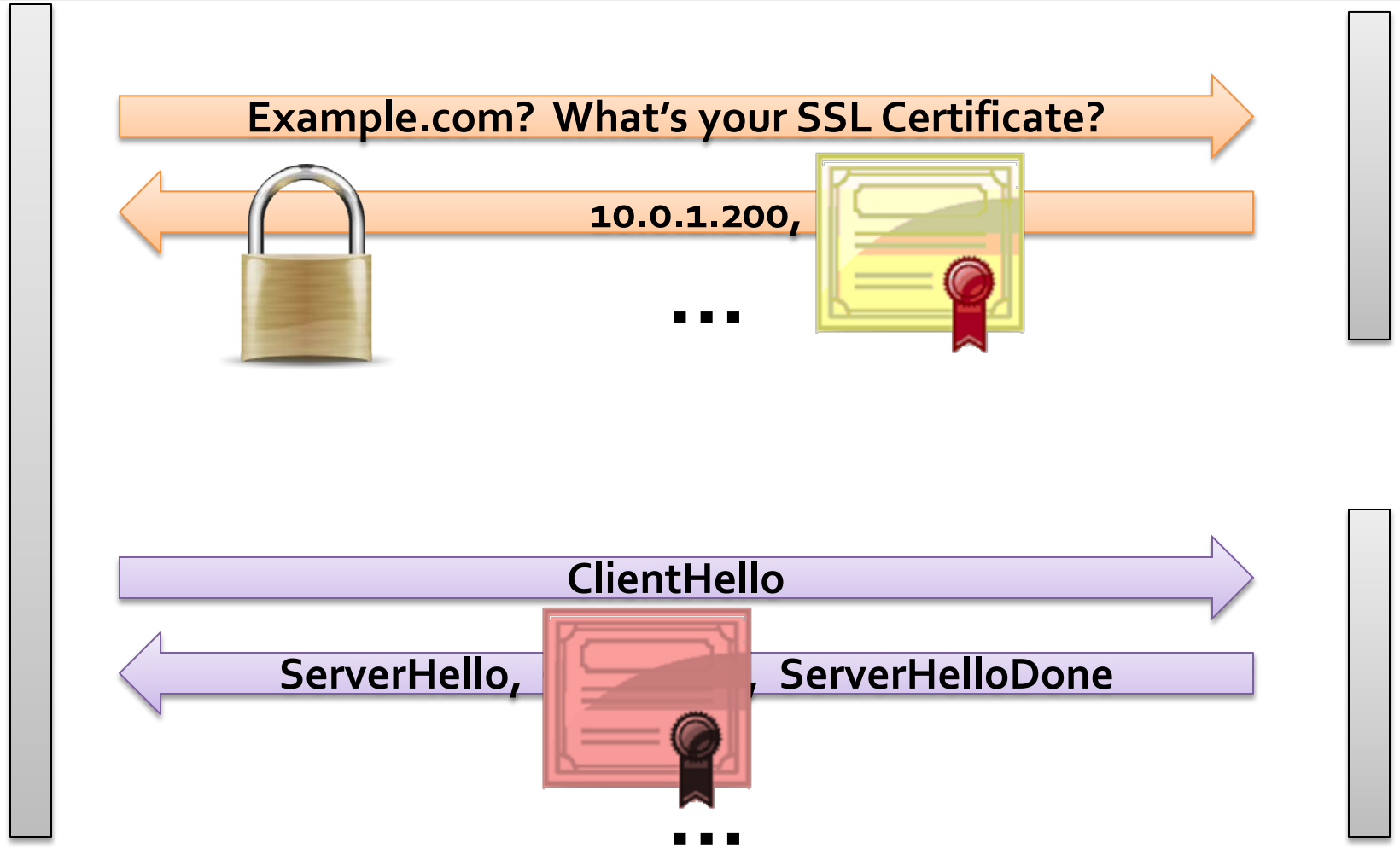
Shoving Stuff in DNSSEC

iSECpartners part of nccgroup





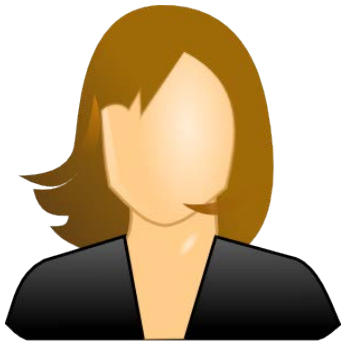
Shoving Stuff in DNSSEC



Shoving Stuff in DNSSEC

iSECpartners part of nccgroup

=



iSECpartners
part of nccgroup

Bootstrapping Security

iSECpartners
part of nccgroup

SSL Certs (DANE)

Product Update Checks

iSECpartners
part of nccgroup

SSL Certs (DANE)

Product Update Checks

SSH

- ssh -o "VerifyHostKeyDNS yes"
- RFC 4255

OpenPGP

- gpg --auto-key-locate pka

S/MIME

- draft-hoffman-dane-smime-03

Domain Policy Framework

iSECpartners part of nccgroup

- Our attempt to unify several DNS security languages into one, extensible meta-language
- Takes advantage of new gTLD program to build special new neighborhood
- Combines a per-gTLD base policy with policy in DNS:

```
Base Policy:       DPFv=1;HTLS=12;DNSSEC=2;STLS=1;
Received Policy:   DPFv=2;HTLS=13;STLS=0;
Resultant Policy:   DPFv=2;HTLS=13;DNSSEC=2;STLS=1;
```

DOMAINPOLICY
working group

DomainPolicy.org

iSECpartners
part of nccgroup

New gTLDs

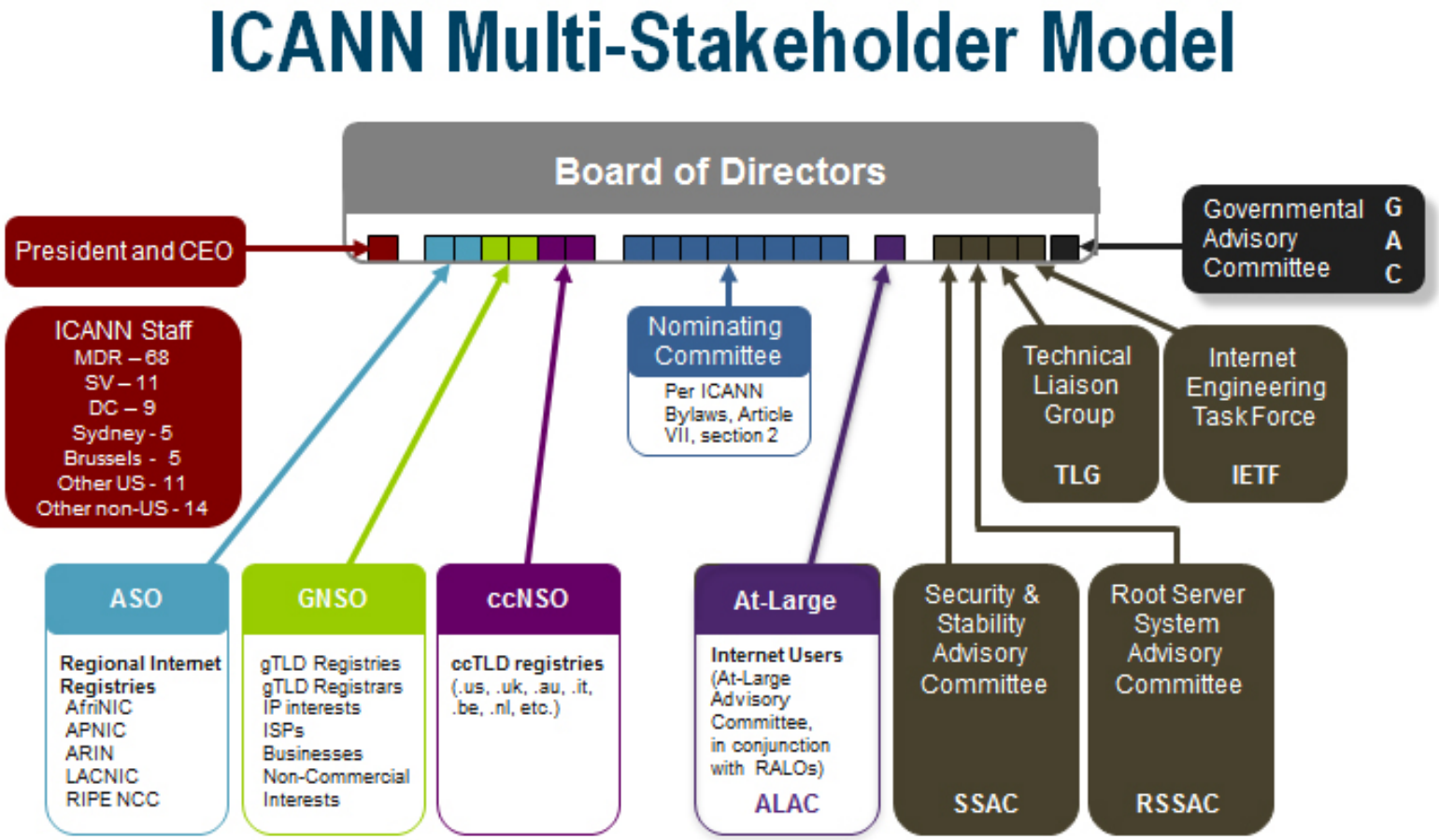
.com .org .net

.biz .museum .coop

.whatever .you .like

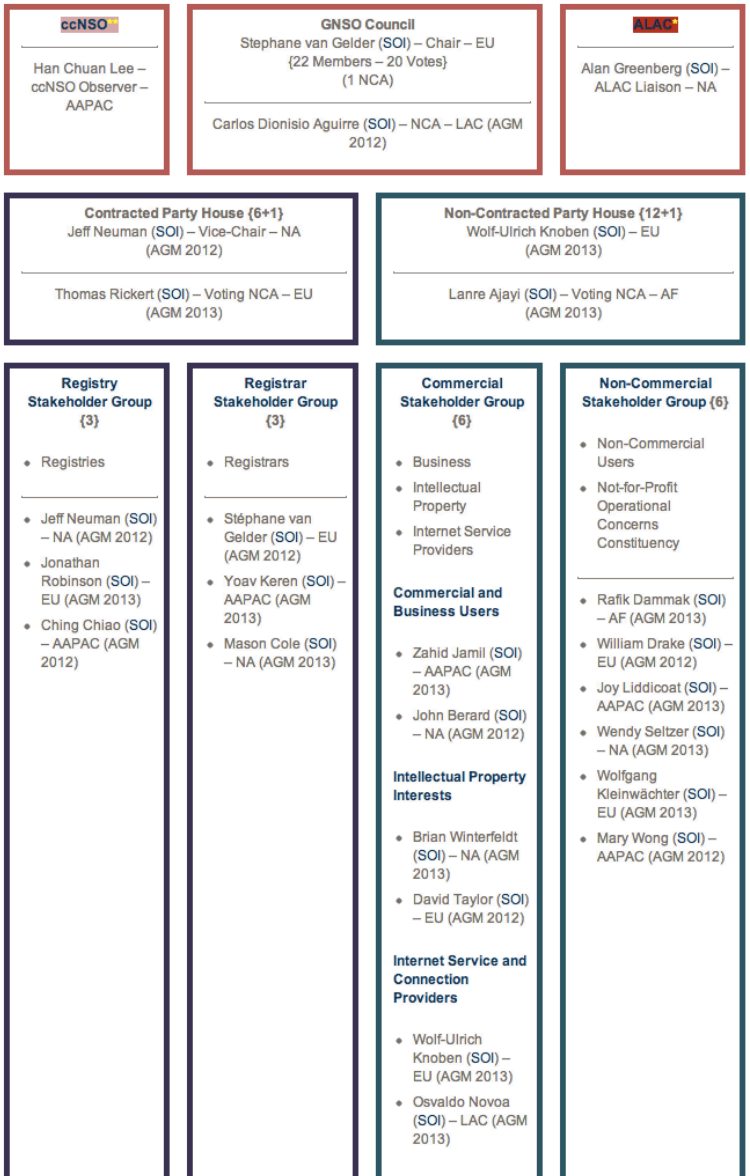
Where ICANN Ended Up

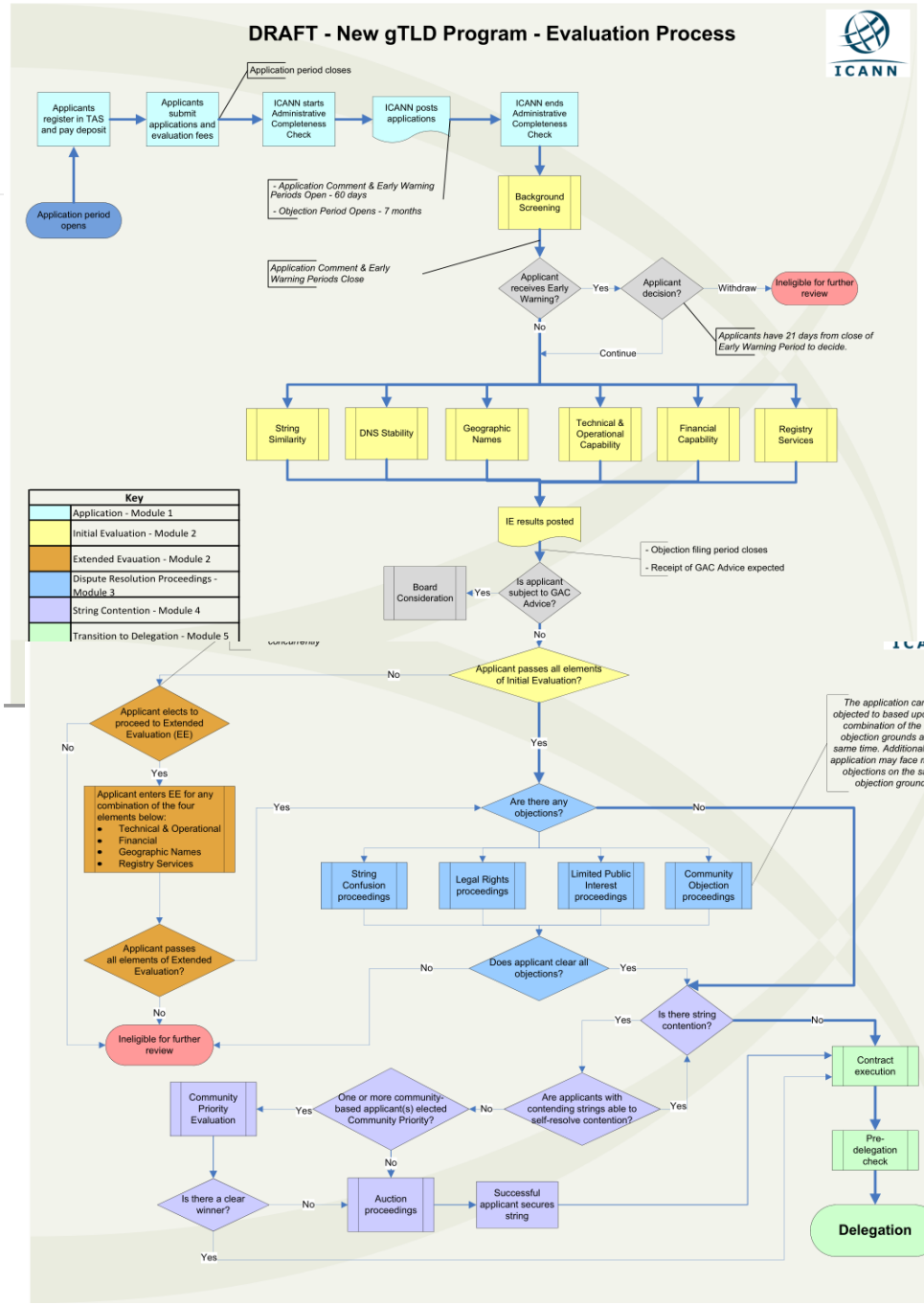
iSECpartners part of nccgroup



Where ICANN Ended Up

iSECpartners part of nccgroup




DRAFT - New gTLD Program - Evaluation Process
ICANN
Application period closes
Applicants register in TAS and pay deposit
Applicants submit applications and evaluation fees
ICANN starts Administrative Completeness Check
ICANN posts applications
ICANN ends Administrative Completeness Check
Application period opens
- Application Comment & Early Warning Periods Open - 60 days
- Objection Period Opens - 7 months
Background Screening
Application Comment & Early Warning Periods Close
Applicant receives Early Warning?
Yes
Applicant decision?
Withdraw
Ineligible for further review
No
Continue
Applicants have 21 days from close of Early Warning Period to decide.
String Similarity
DNS Stability
Geographic Names
Technical & Operational Capability
Financial Capability
Registry Services
Key
Application - Module 1
Initial Evaluation - Module 2
Extended Evauation - Module 2
Dispute Resolution Proceedings - Module 3
String Contention - Module 4
Transition to Delegation - Module 5
IE results posted
- Objection filing period closes
- Receipt of GAC Advice expected
Board Consideration
Yes
Is applicant subject to GAC Advice?
No
ICANN
No
Applicant passes all elements of Initial Evaluation?
Applicant elects to proceed to Extended Evaluation (EE)
No
Yes
Yes
Applicant enters EE for any combination of the four elements below:
Technical & Operational
Financial
Geographic Names
Registry Services
Are there any objections?
Yes
No
The application can be objected to based upon any combination of the four objection grounds at the same time. Additionally, the application may face multiple objections on the same objection ground.
String Confusion proceedings
Legal Rights proceedings
Limited Public Interest proceedings
Community Objection proceedings
Applicant passes all elements of Extended Evaluation?
No
Does applicant clear all objections?
Yes
No
Yes
Is there string contention?
Yes
No
Ineligible for further review
Contract execution
Community Priority Evaluation
Yes
One or more community-based applicant(s) elected Community Priority?
No
Are applicants with contending strings able to self-resolve contention?
Yes
Pre-delegation check
No
Is there a clear winner?
No
Auction proceedings
Successful applicant secures string
Delegation
Yes

.bugatti

iSECpartners
part of nccgroup

Competition and Public Interest

iSECpartners part of nccgroup

Competition and Public Interest

iSECpartners part of nccgroup

Most new gTLDs could be closed shops

Kevin Murphy, June 21, 2012, Domain Registries

ICANN's new generic top-level domain program could create almost 900 closed, single-user namespaces, according to DI PRO's preliminary analysis.

Surveying all 1,930 new gTLD applications, we've found that 912 – about 47% – can be classified as "single registrant" bids, in which the registry would tightly control the second level.

Single-registrant gTLDs are exempt from the Registry Code of Conduct, which obliges registries to offer their strings equally to the full ICANN-accredited registrar channel.

The applications include those for dot-brand strings that match famous trademarks, as well as attempts by applicants such as Amazon and Google to secure generic terms for their own use.

Amazon.com's domain power play: We want to control them all

The e-commerce giant is applying for 76 new top-level domains -- and you won't be able to register any of them. What exactly does it have up its sleeve?

by Paul Sloan | June 21, 2012 4:00 AM PDT

Follow @paulsloan

If Amazon.com gets its way -- and that's still a big "if" -- it will soon control 76 new domain extensions on the Internet. Most observers had expected the company to apply for .amazon and .kindle, but it seems that was just for starters: Amazon's ambitions also include a host of generic terms, including the likes of .free, .like, .game, and .shop.

06|19|2012 06:12 pm EDT

New gTLDs: Competition or Concentration? Innovation or Domination?

by Phil Corwin in Categories: new gTLDs

This guest post was writting by Phil Corwin. Mr. Corwin is Founding Principal of the Virtualaw LLC consultancy and serves as Of Counsel to Greenberg & Lieberman and as for the Internet Commerce Association (ICA), all located in Washington, DC. This post is his personal opinion.

Expect the unexpected. Because it will happen. And it has just happened in the application phase of ICANN's new gTLD program, with potentially profound consequences for the future of e-commerce.

During the three year period between the June 2008 ICANN Board approval of the new gTLD program and its June 2011 vote to proceed to the application stage, and even beyond then in the context of continuing GAC-Board discussions, only one competition issue ever became the subject of heated and protracted debate. And that was whether ICANN's requirement for registry-registrar separation should be relaxed in concert with the new gTLD program, a question that ICANN eventually answered in the affirmative notwithstanding resistance from some members of the GAC.

Top Level Websites

iSECpartners part of nccgroup

- Supposed to be outlawed
- How do you represent them
  - http://ai
  - http://ai.
  - http://ai/
- How does this interact with certificate authorities?
  - We could have bought *.bugatti for less than $10K

Existing A records:

- AC has address 193.223.78.210
- AI has address 209.59.119.34
- BT has address 192.168.42.202
- CM has address 195.24.205.60
- DK has address 193.163.102.24
- GG has address 87.117.196.80

iSECpartners
part of nccgroup

The Big Picture

- The Death of Reputation
- Redesigning Enterprise Networks and Attacks
- External Attacks and Enumeration
- Product Promises and Failures

The End of Scarcity

iSECpartners
part of nccgroup

The Death of Reputation

iSECpartners part of nccgroup

Scarcity makes certain assumptions reasonably true:

- An individual user has a high attachment rate for a small number of IPs
- A trademarked domain name has likely been taken by the most recognizable holder
- IP spoofing is highly limited in full-connection situations

Uses of IP Reputation

iSECpartners part of nccgroup

- Anti-Fraud and Adaptive Authentication
  - RSA, SilverTail, EnTrust
- DDoS Prevention and Rate Limiting
  - Arbor Networks, RadWare, every load balancer
- IDS, SIEM and Event Correlation
  - ArcSight, Splunk, Sourcefire

A simple example:

```
rate_filter
        gen_id 135, sig_id 1,
        track by_src,
        count 100, seconds 1,
        new_action drop, timeout 10
```

Per IP

How can you Adapt?

iSECpartners part of nccgroup

Switch to "Network Reputation"

- Intelligent detection of subnetting
- Correlation to other data to determine flows
- Positive, not negative reputation
- Con: One bad actor could DoS a popular network
- Con: State table will need to be ginormous, creates another DoS

Filter out network bogons

- Reverse BGP lookups
- Central databases of assigned and utilized spaces

Implement intelligent egress filtering

- Subnet limits no longer good enough, need stateful tracking of assigned IPs

Domain Reputation

iSECpartners part of nccgroup

- A lot of security thinking goes into securing this relationship:

www.paypal.com <-> 173.0.84.2

- This is also an important mapping:

www.paypal.com <-> The Real PayPal with all the Money

- With 1400 potential new gTLDs, this mapping becomes more difficult for consumers to keep in their head

WhoTF is paypal.rugby?

Domain Reputation Protection

iSECpartners part of nccgroup

- ICANN nGTLD Rules
  - You need to be heavily engaged right now, coming to ICANN meetings
  - Should be possible to derail .yourbrand via official objection process
- Trademark Clearing House
  - Required part of first 90 days of registration
  - Any trademark works, rules and implementation are in flux
- Sunrise Period
  - Required window for existing gTLD and trademark owners to step to the front of line
  - Easiest and cheapest way to get your gTLD
  - Only lasts 30 days, you'll need to be ready
- URS
  - Mechanism for suspending (but not taking) second level domains
  - Much more IP-friendly than existing WIPO process
  - Nobody wants to run this for $500/name

A word you will hear often

iSECpartners part of nccgroup

Homograph!

http://paypal.com

xn--fsqu00a.xn—g8w231d

http://paypal.com

xn--fsqu00a.xn--g6w251d

PunyCode

iSECpartners part of nccgroup

http://مثال.إختبار

xn--mgbhofb.xn--kgbechtv

http://例子.測試

xn--fsqu00a.xn--g6w251d

http://пример.испытание

xn--e1afmkfd.xn--80akhbyknj4f

http://דוגמה.טעסט

xn--fdbk5d8ap9b8a8d.xn--deba0ad

Browser Homograph Handling

iSECpartners part of nccgroup

Internet Explorer

- System language settings
- Does not allow mixed characters

Chrome

- Browser language settings
- Does not allow mixed character sets

Firefox

- Whitelists TLDs, changing

Opera

- Whitelists TLDs

Safari…

Safari Character White List

iSECpartners part of nccgroup

IDNScriptWhiteList.txt — Locked

```
# Default Web Kit International Domain Name Script White List.

Common
Inherited

Arabic
Armenian
Bopomofo
Canadian_Aboriginal
Devanagari
Deseret
Gujarati
Gurmukhi
Hangul
Han
Hebrew
Hiragana
Katakana_Or_Hiragana
Katakana
Latin
Tamil
Thai
Yi
```

Enterprise Architecture

iSECpartners part of nccgroup

IPv6 is intended to restore the "end-to-end principal"

Will it?

True IPv6 Enterprises would include:

1. Publicly addressable end-points
2. Firewalls doing actual firewalling
3. NAT64 mechanisms for IPv4 access
4. VPN with sticky addresses, like DirectAccess

Will this happen?

iSECpartners part of nccgroup

Probably not… more likely:

1. Mix of real IPv6 and NAT

- Both IP versions running end-to-end for a while, causing lots of access control headaches
- Large scale NAT64 for native IPv6 clients

2. Lots of public addressing with private routing

- Using a real prefix doesn't mean you allow public routing.
- Controls should include null route tables for specific subnet netmask and firewall rules

3. Proxies will become even more important for egress control

- Proliferation of network identities makes it important to create artificial checkpoints
- Proxies can provide authentication and logging not based on IP4/6 address

Pros and Cons for Attackers

iSECpartners part of nccgroup

Pros:

- Likelihood of routable end-points that can be attacked directly (80's style)
- ARP Spoofing becomes at least 6 new link local attacks
- Easier to hide attacks, internal compromised machines, control channels
- Multiple IP identities slows down incident response

Cons:

- Finding machines via random IP scanning impossible
- 100% coverage of routable space not possible
- DNSSEC provides some protections if properly deployed

Future Work

iSECpartners part of nccgroup

You should submit these talks to BlackHat USA 2013:

- "Denial of Service via IPv6 State Exhaustion"
- "Using and Abusing IPv6 Multicast for Fun and Profit"
- "I Want All the Internets: Hacking with Translation and Transition Mechanisms"
- "This Crap Broke: A Study of Major Vendor Products in an all IPv6/DNSSEC World"
- "IPv6 Covert Channels"

iSECpartners
part of nccgroup

Thank You

Alex Stamos

alex@artemis.net

Artemis Internet

Tom Ritter

tritter@isecpartners.com

iSEC Partners