

DNSSEC: Securing an “In-secure” Medium

Shernon Osepa

Manager, Regional Relations Caribbean



St. Kitts and Nevis CTU's Roadshow

St. Kitts, 16 June 2011

Agenda

- What is ICANN?
- The Domain Names System (DNS)
- DNSSEC
- DNSSEC ccTLD signing initiative
- Q & A

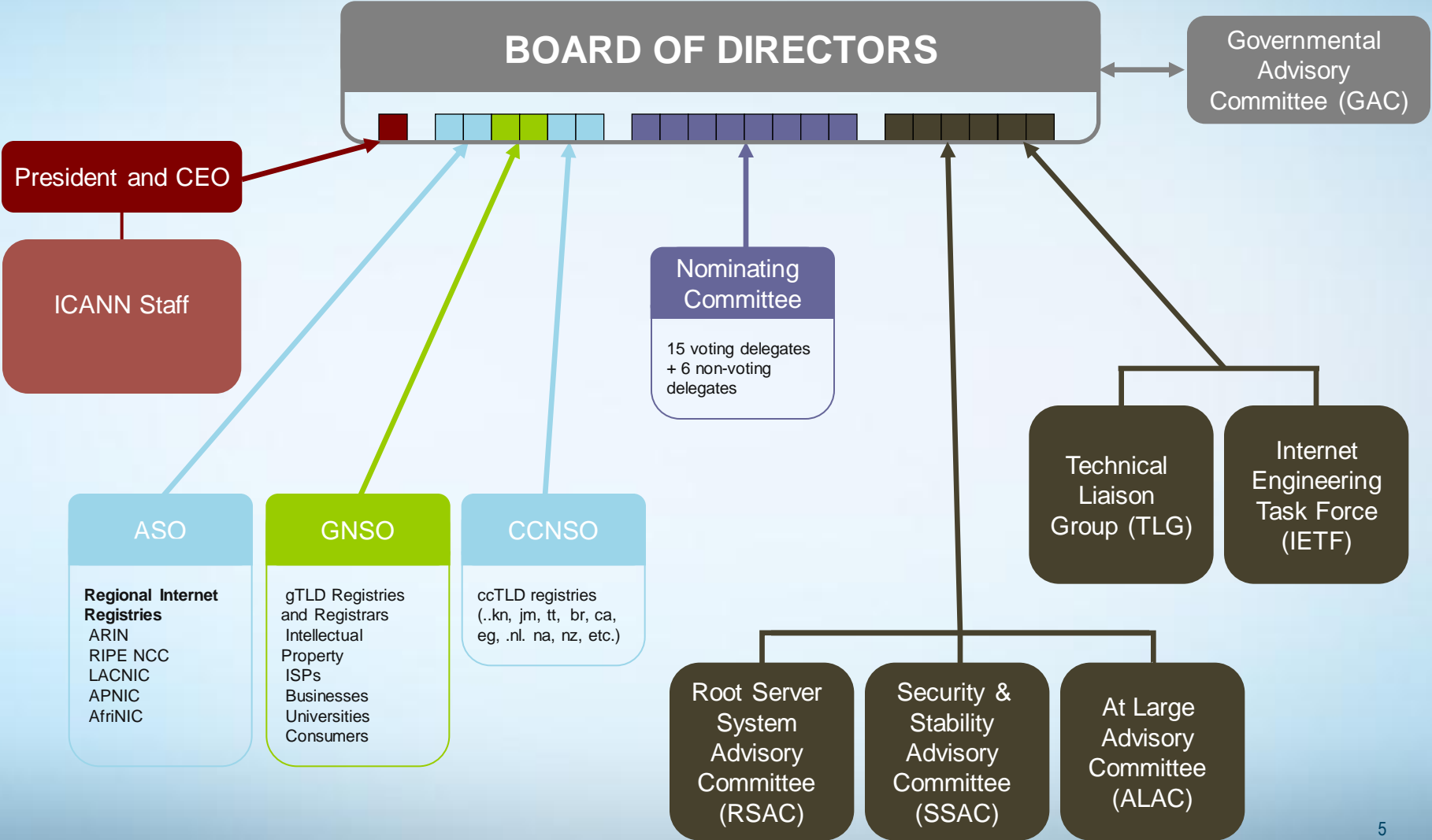
ICANN' s role

- Internationally organized, non-profit organization that has responsibility for IP address space allocation, protocol identifier assignment, gTLDs and ccTLDs name system management and root server coordination
- Is dedicated to preserving the operational stability of the Internet
- (Not) rules for financial transactions, content control, spam, data protection

How does ICANN work?

- Bottom-up consensus building model
 - Governments
 - Private sector
 - Technical community
 - Users
- Internationally diverse Board of Directors overseeing the policy development process
- President & CEO, staff

ICANN's Community



Accomplishments and ongoing work

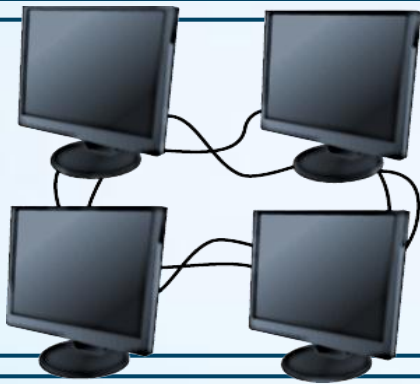
- Established market competition for gTLDs
- Implemented a UDRP (>5000 disputes regarding trademark rights resolved)
- New gTLDs (.aero,.biz, .coop,.info, .museum,.name,.pro,.mobi,.tel) others are being explored (ongoing process)
- Workshops on relevant issues (gTLDs, IDNs, IPv6,etc)
- AoC post JPA
- IDNs

ICANN welcomes participation

- End users
 - Participation in At Large
- ccTLDs
 - Participation in ccNSO and AF/EoL
- Governments
 - Participation in GAC
- Private sector
 - Registrar accreditation / new gTLDs, IDNs

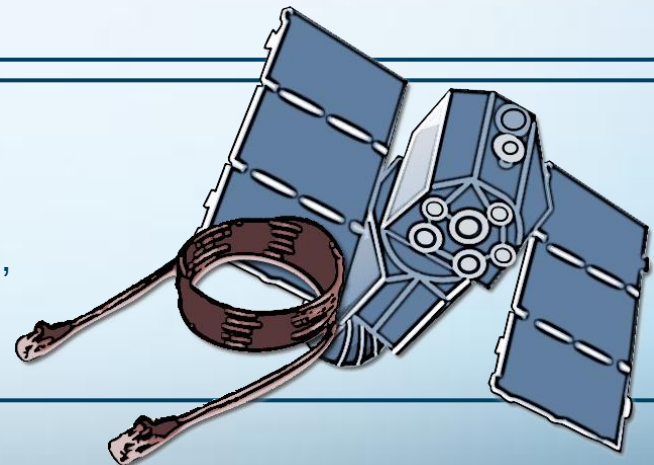
Internet's Three Operating Layers

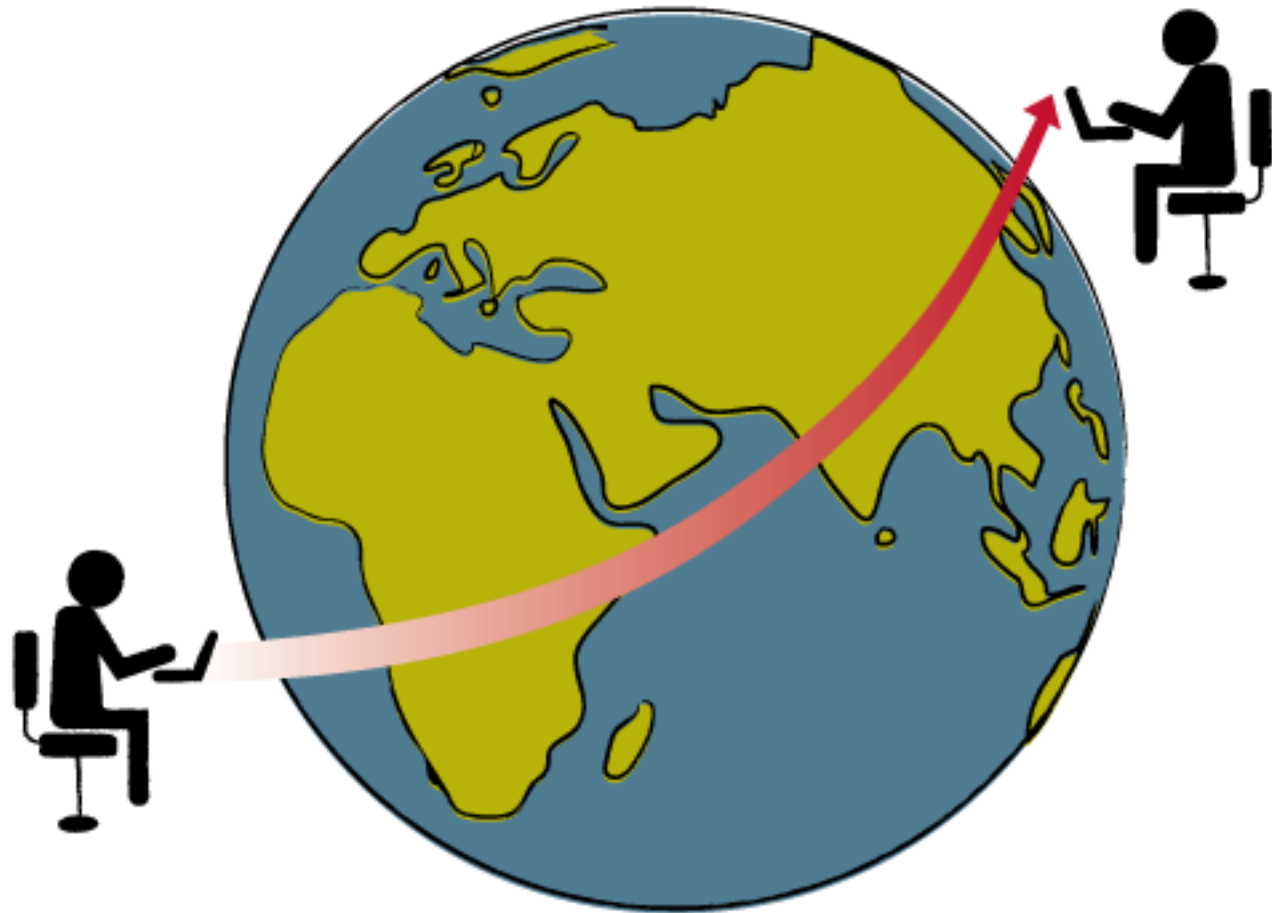
Content and applications standards (HTML, XML, Java) – Promotes creativity and innovation in applications leading to email, World Wide Web, ebanking, wiki, Skype, Yahoo, Google, YouTube and much more



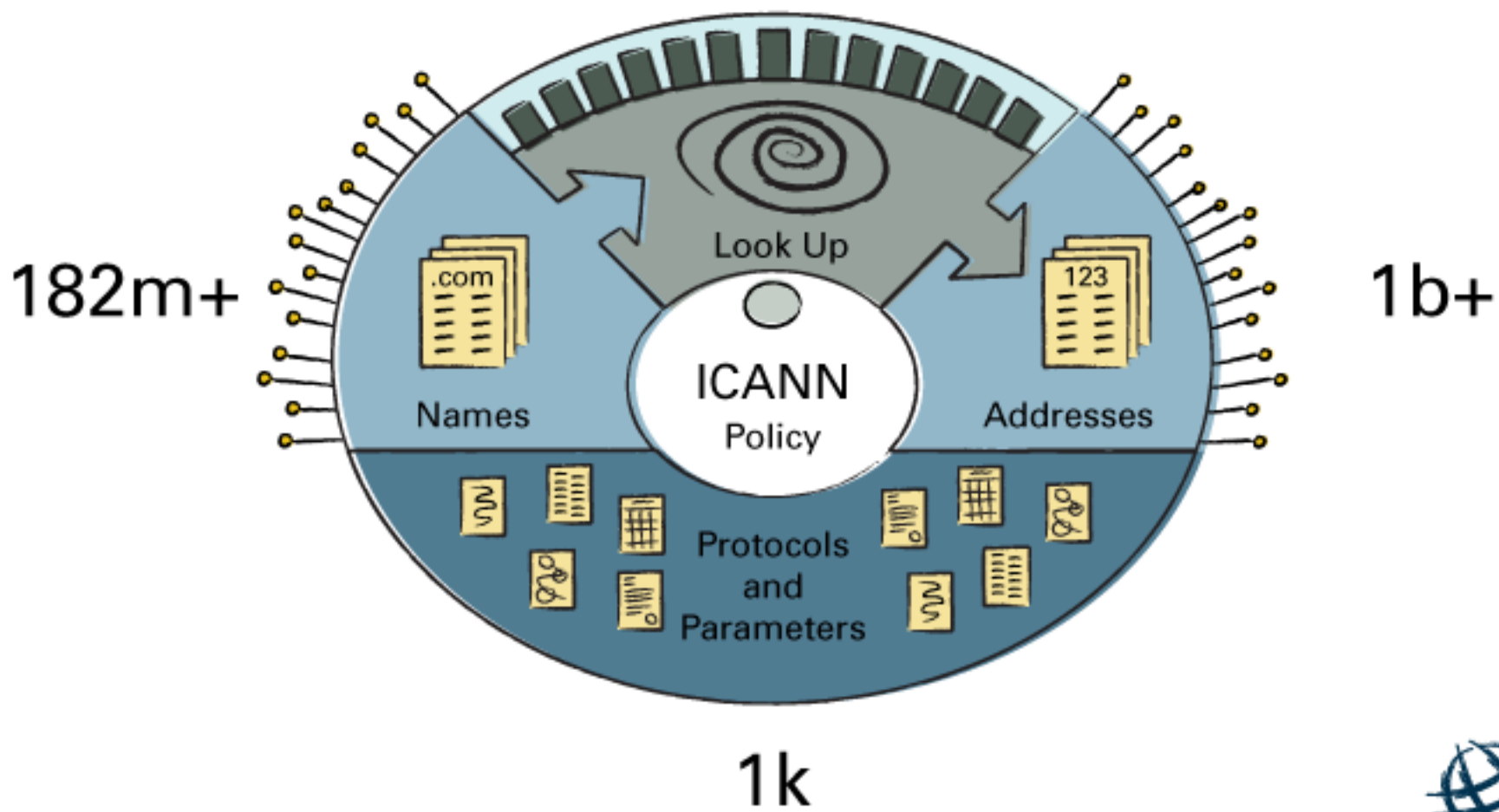
Internet protocols and standards (TCP/IP, DNS, SSL) – TCP/IP, controls traffic flow by dividing email and web data into packages before they are transmitted on the Internet

Telecommunications infrastructure – Physical network made up of underwater cables, telephone lines, fiber optics, satellites, microwaves, wi-fi, and so on Facilitates transfer of electronic data over the Internet



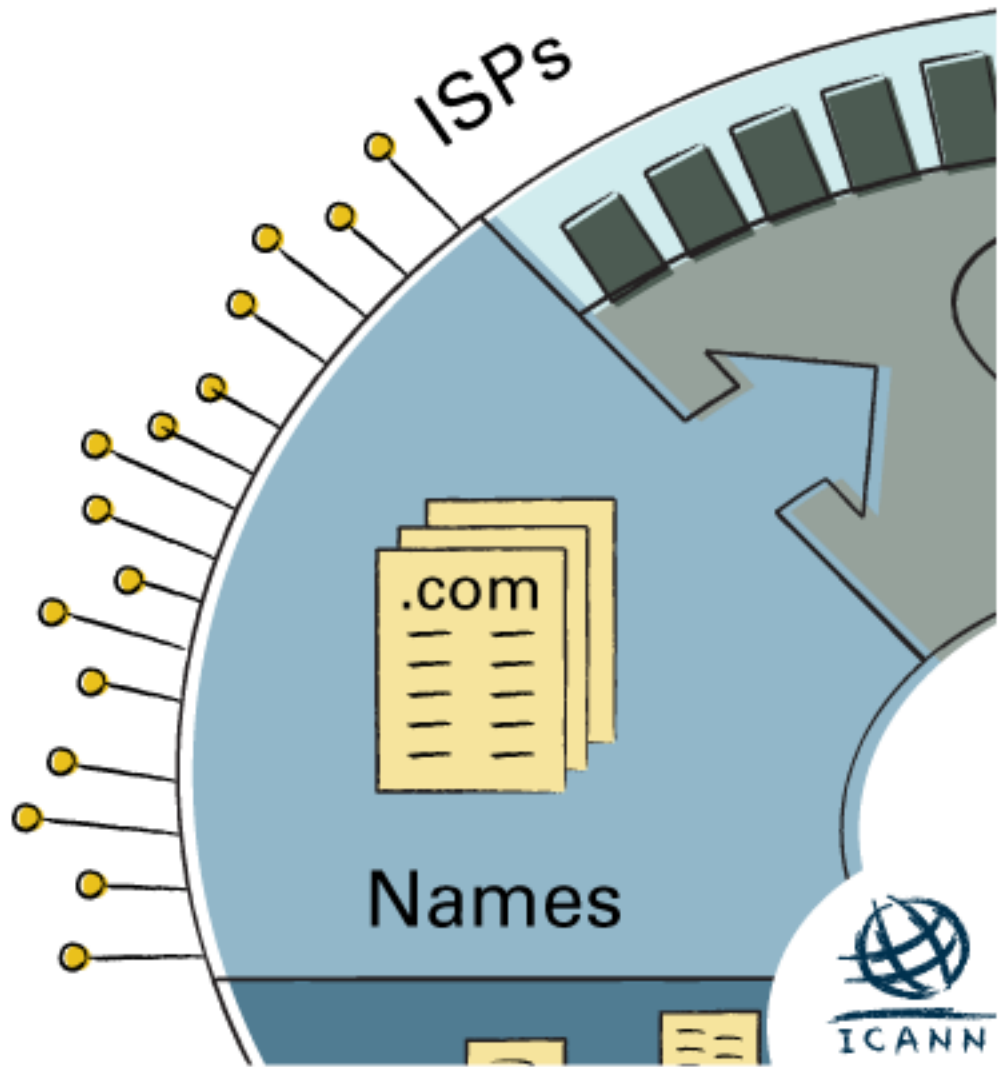


100's of BNs per day



269 Registries

- .org
- .uk
- .net
- .ca
- .me
- .ck
- .au
- .edu
- .fr
- .cn
- .gov
- .biz
- .eg
- .jp
- etc



Register.com

GoDaddy

935 Registrars

269 Registries

- .org
- .uk
- .net
- .ca
- .me
- .ck
- .au
- .edu
- .fr
- .cn
- .gov
- .biz
- .eg
- .jp
- etc

ISPs

.com

Names



Register.com

GoDaddy

935 Registrars

269 Registries
.org
.uk
.net
.ca
.me
.ck
.au
.edu
.fr
.cn
.gov
.biz
.eg
.jp
etc

Registrants

Individuals

Corporations

ISPs



Names



Register.com

GoDaddy

935 Registrars

269 Registries

.org
.uk
.net
.ca
.me
.ck
.au
.edu
.fr
.cn
.gov
.biz
.eg
.jp
etc

Registrants

Individuals

Corporations

ISPs

.com

Names



Register.com

GoDaddy

935 Registrars

269 Registries

- .org
- .uk
- .net
- .ca
- .me
- .ck
- .au
- .edu
- .fr
- .cn
- .gov
- .biz
- .eg
- .jp
- etc

Registrants

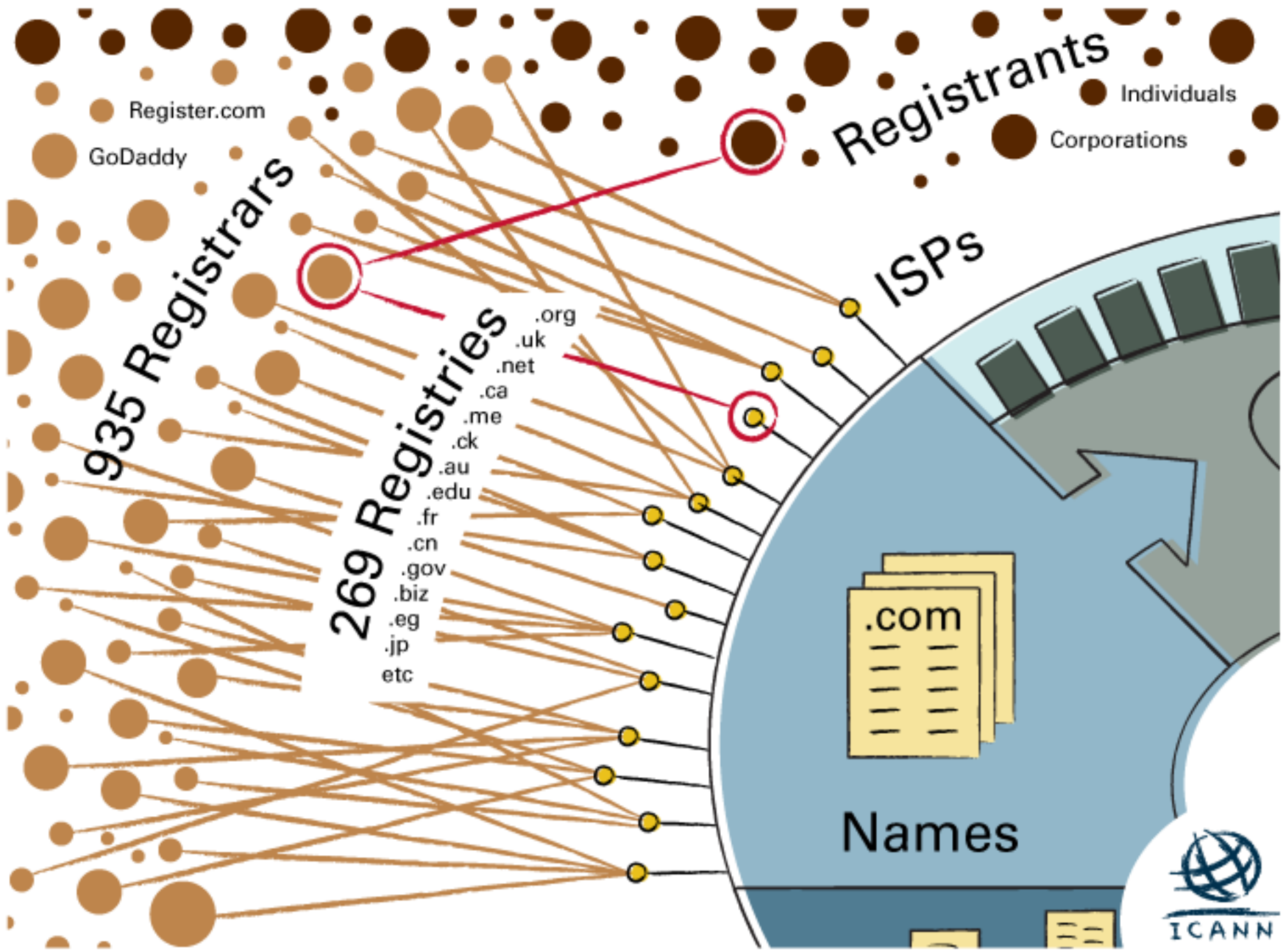
Individuals

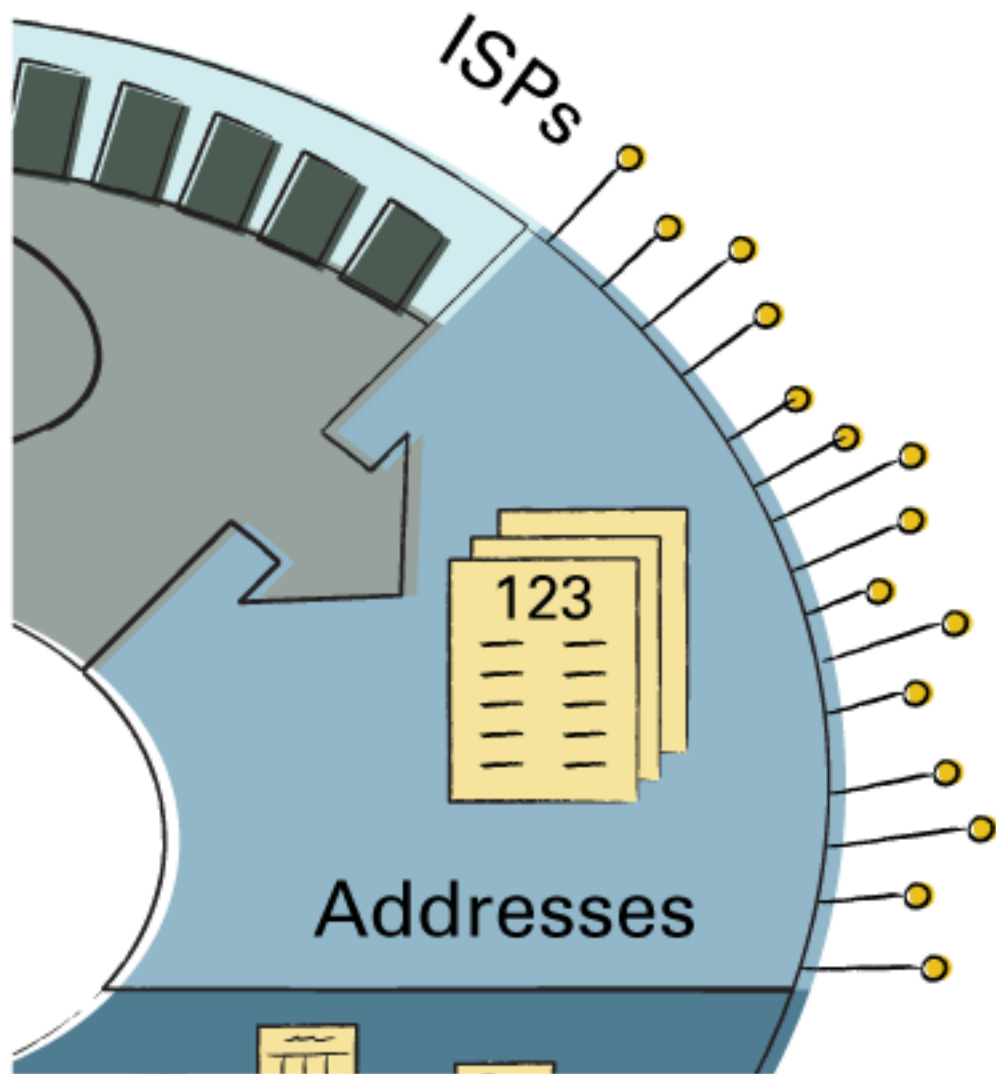
Corporations

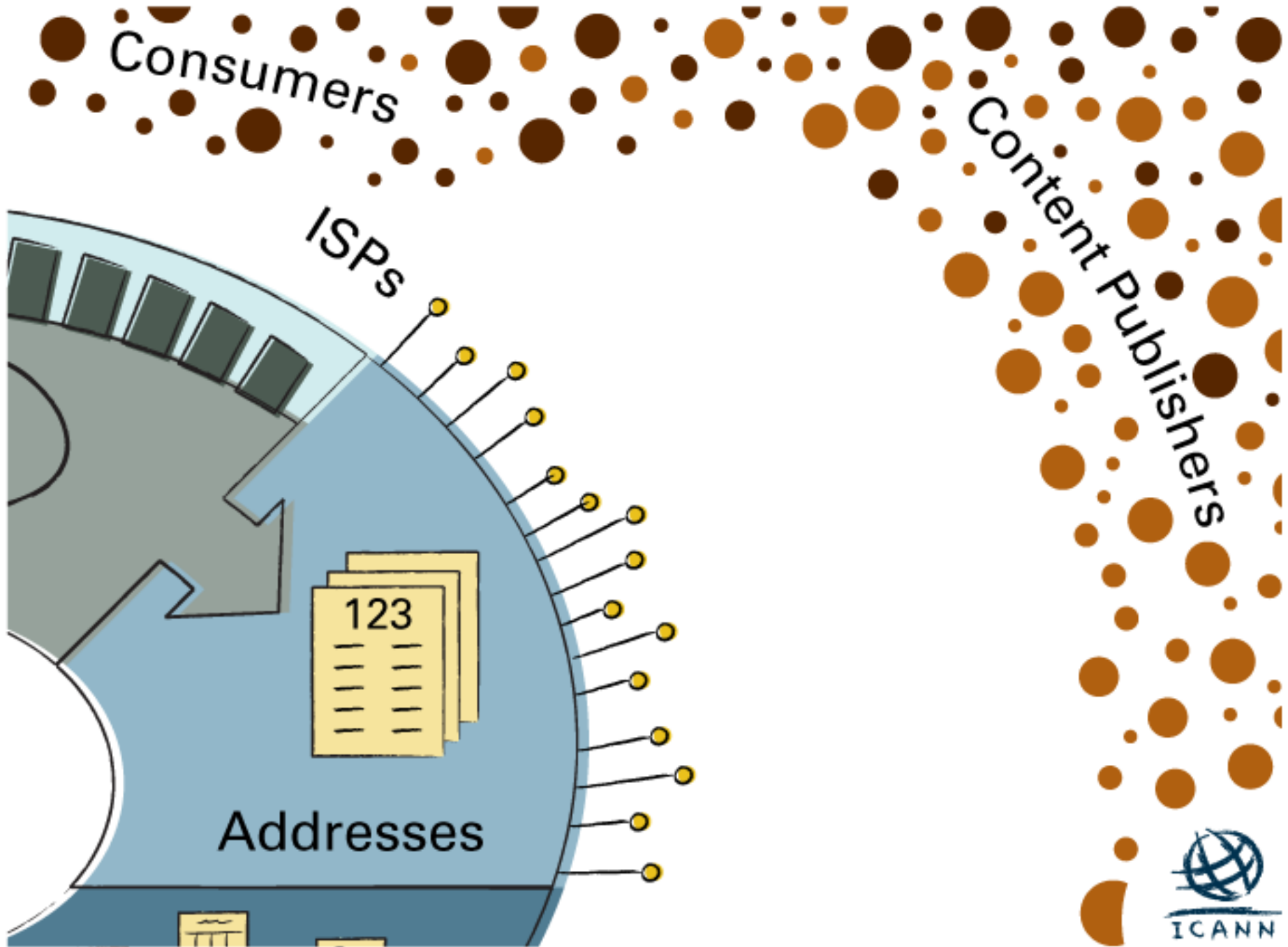
ISPs

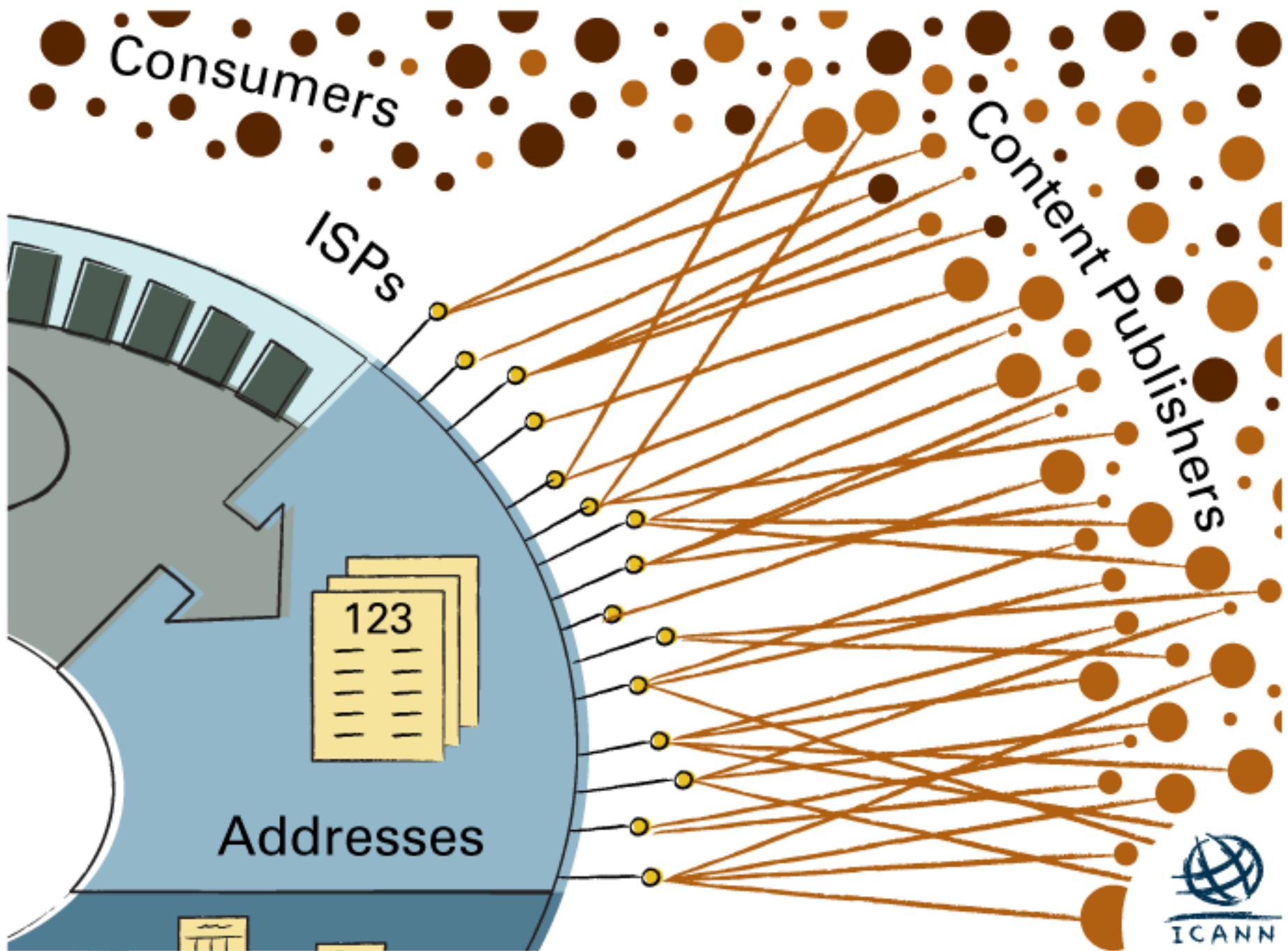


Names



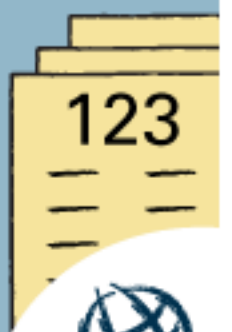


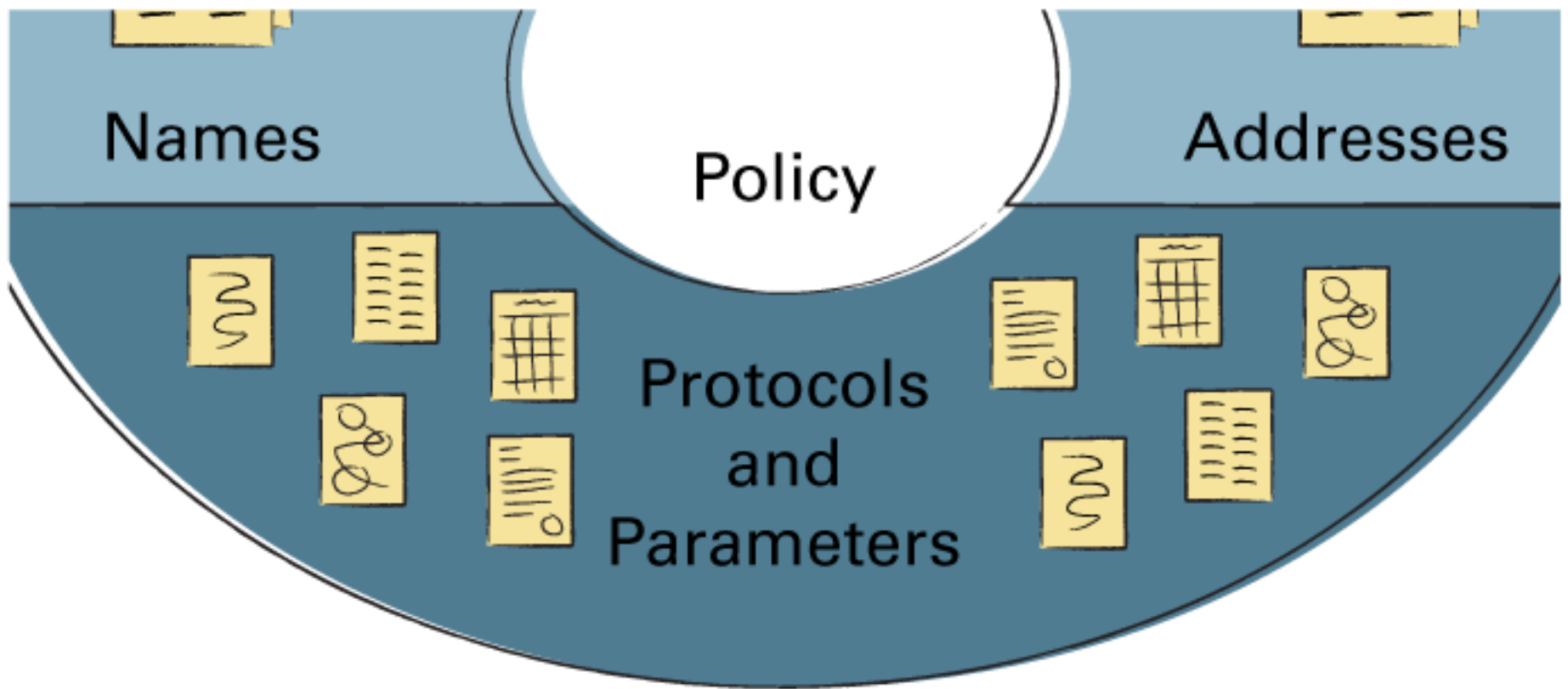


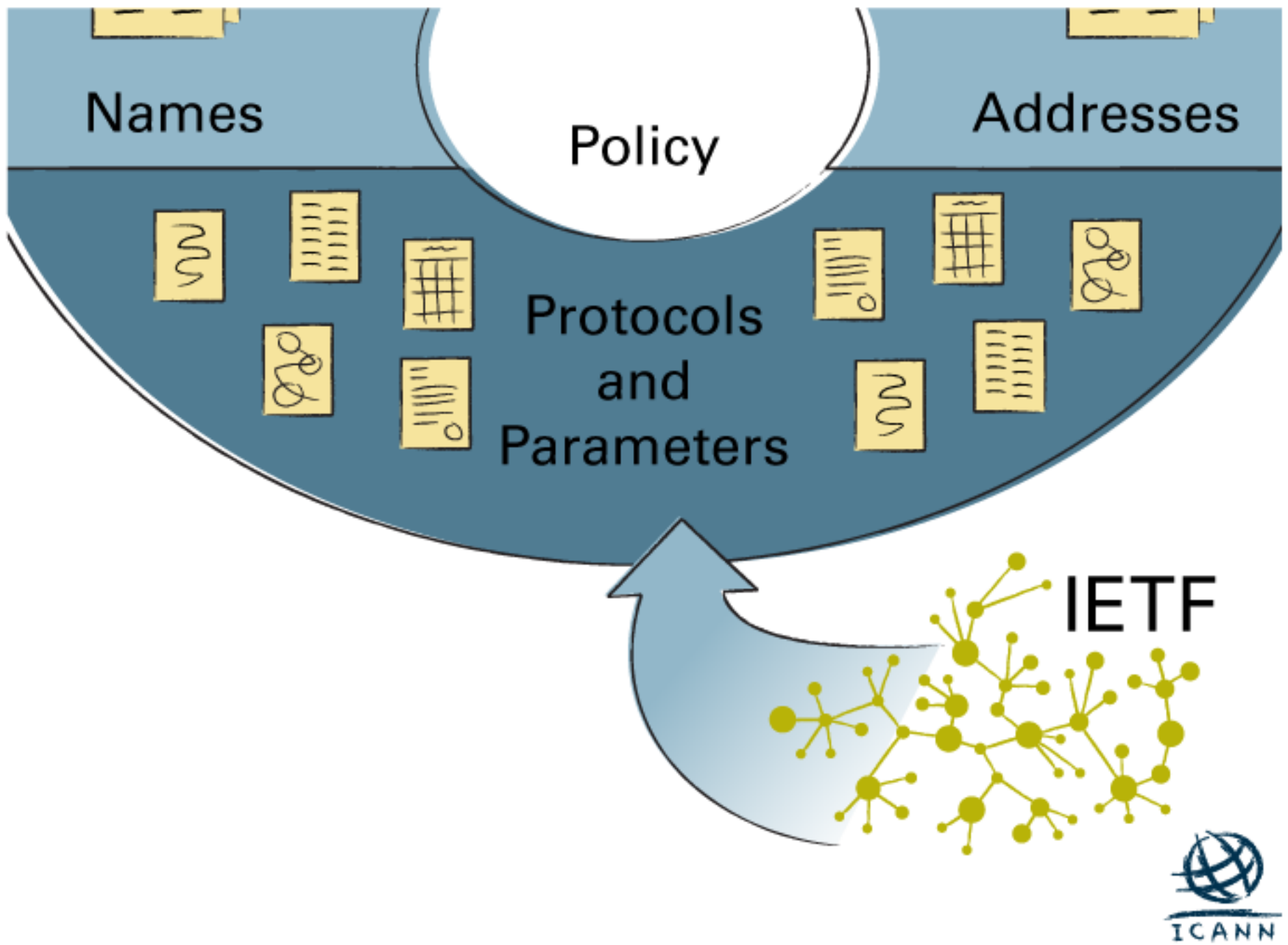


Root Server Operators

Look Up







Names

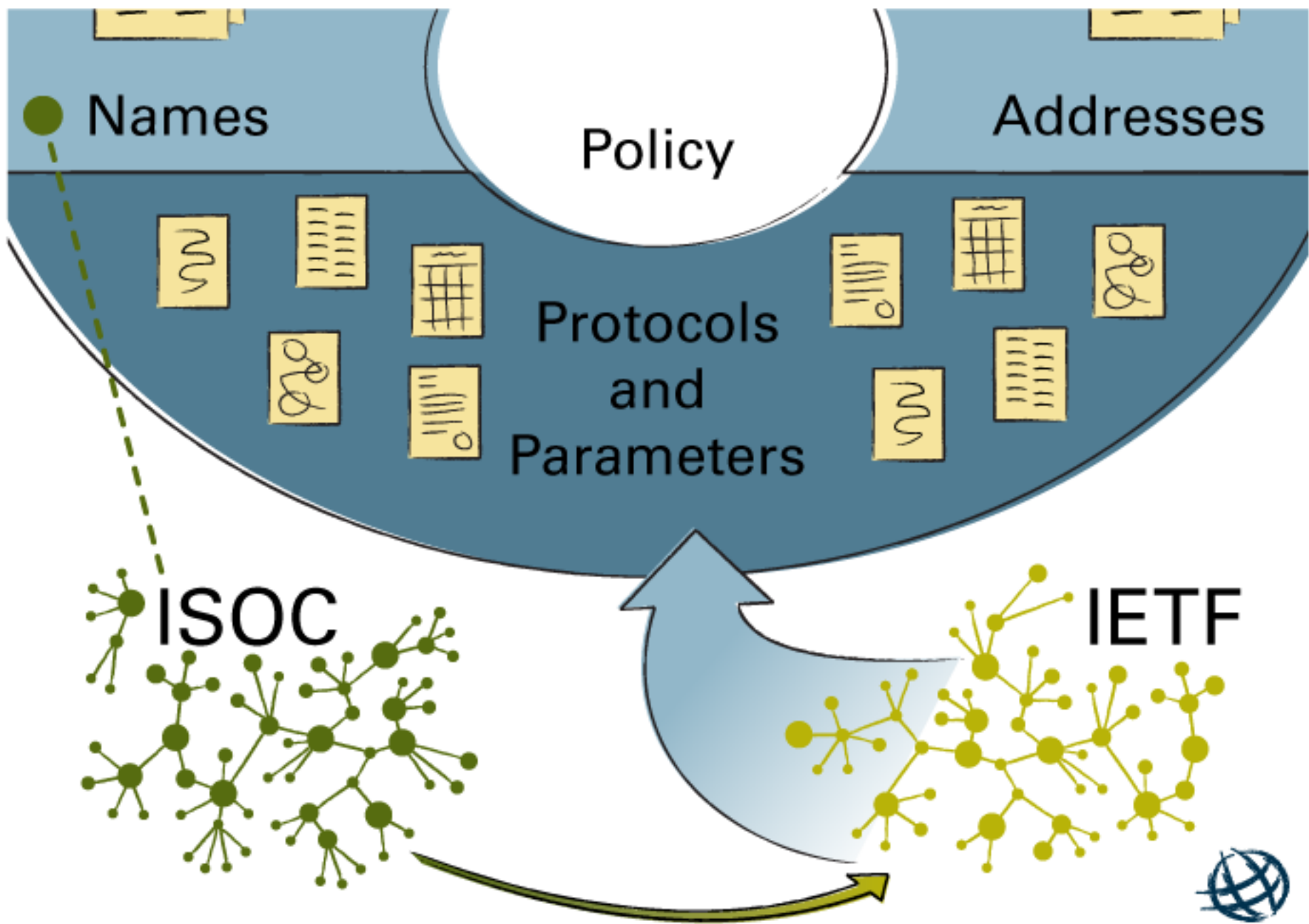
Policy

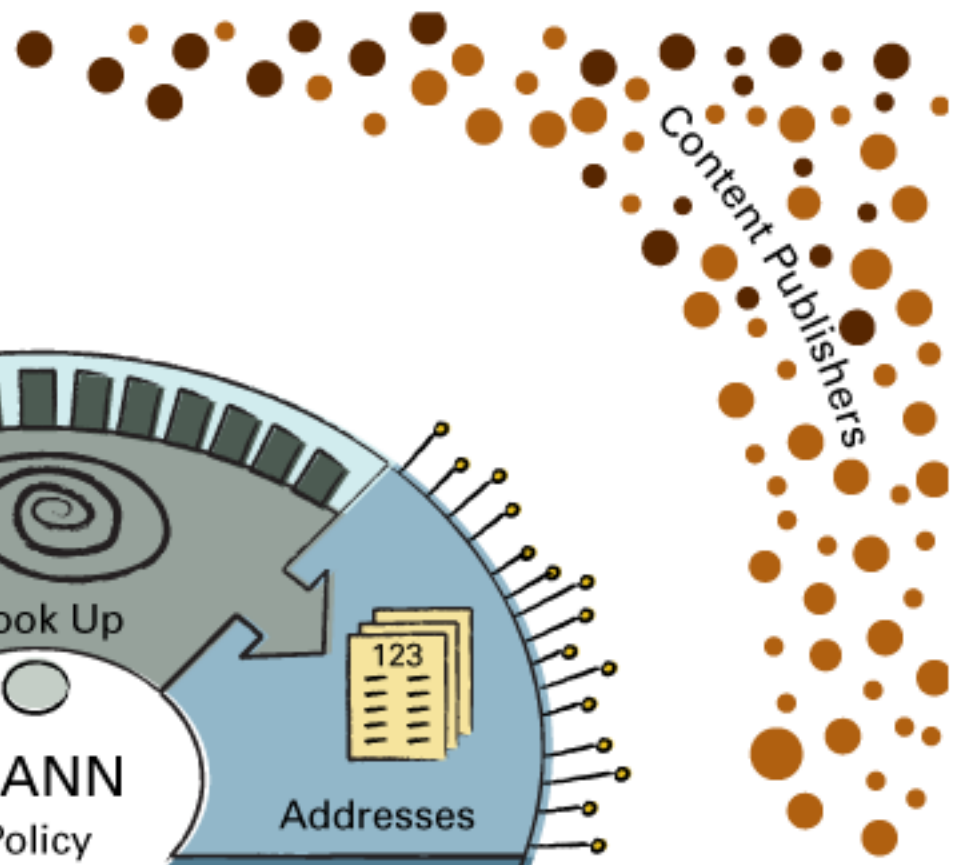
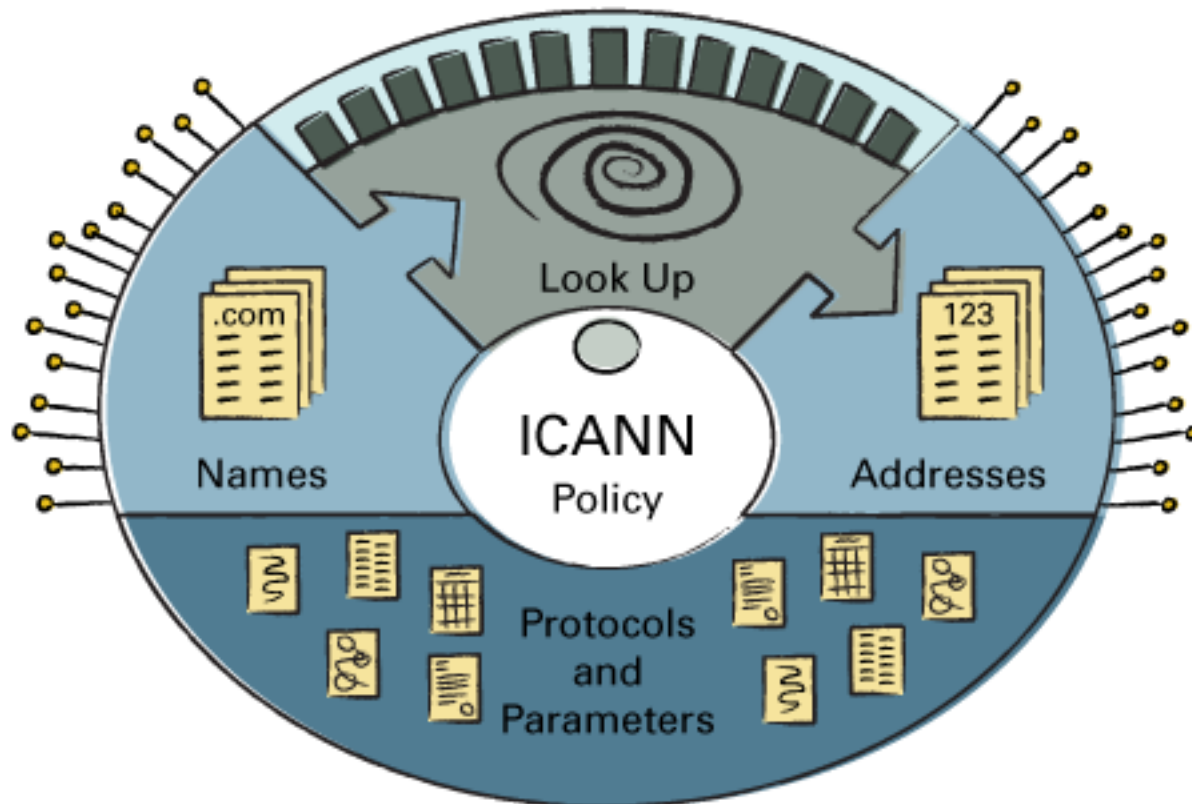
Addresses

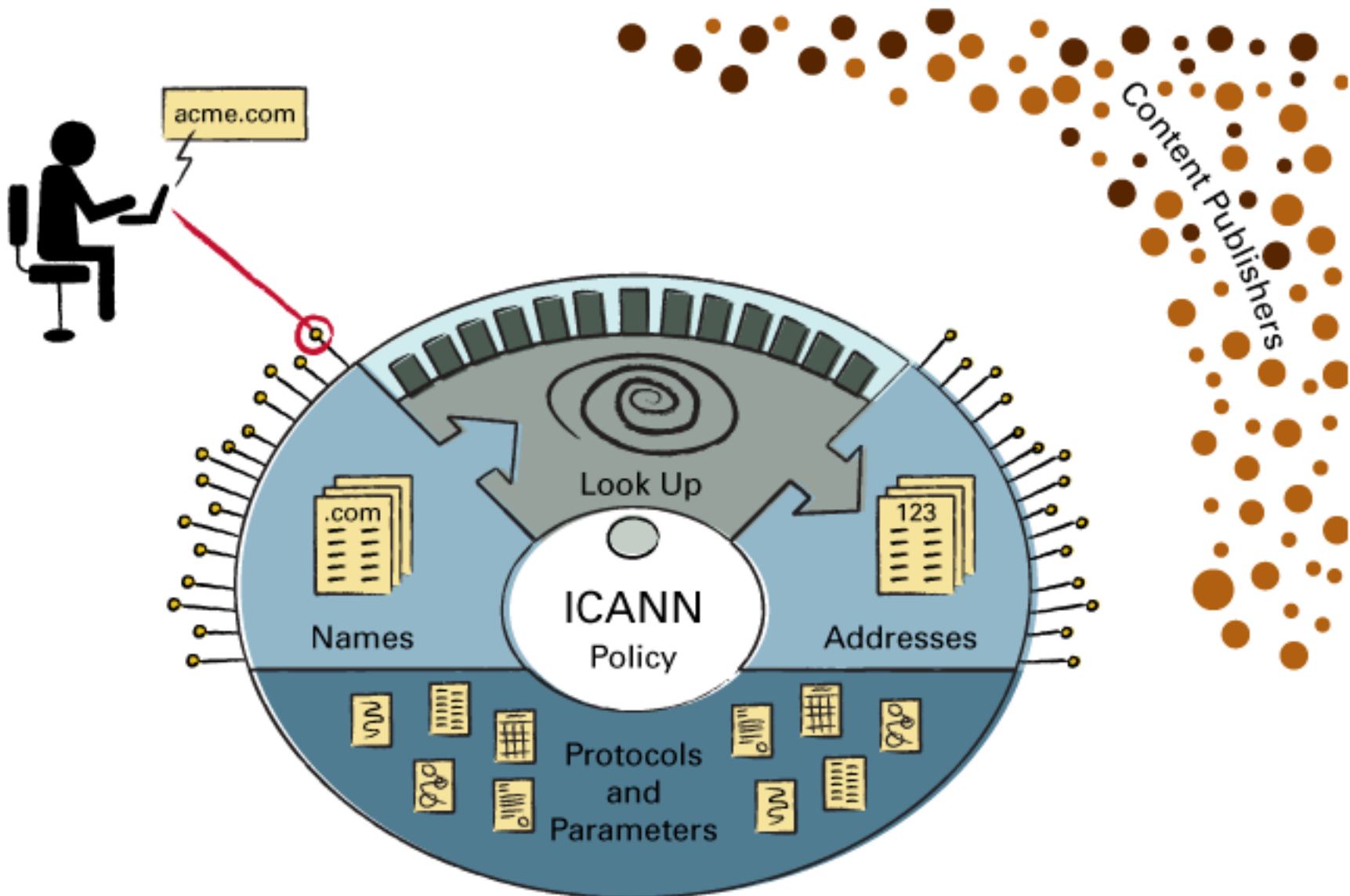
Protocols
and
Parameters

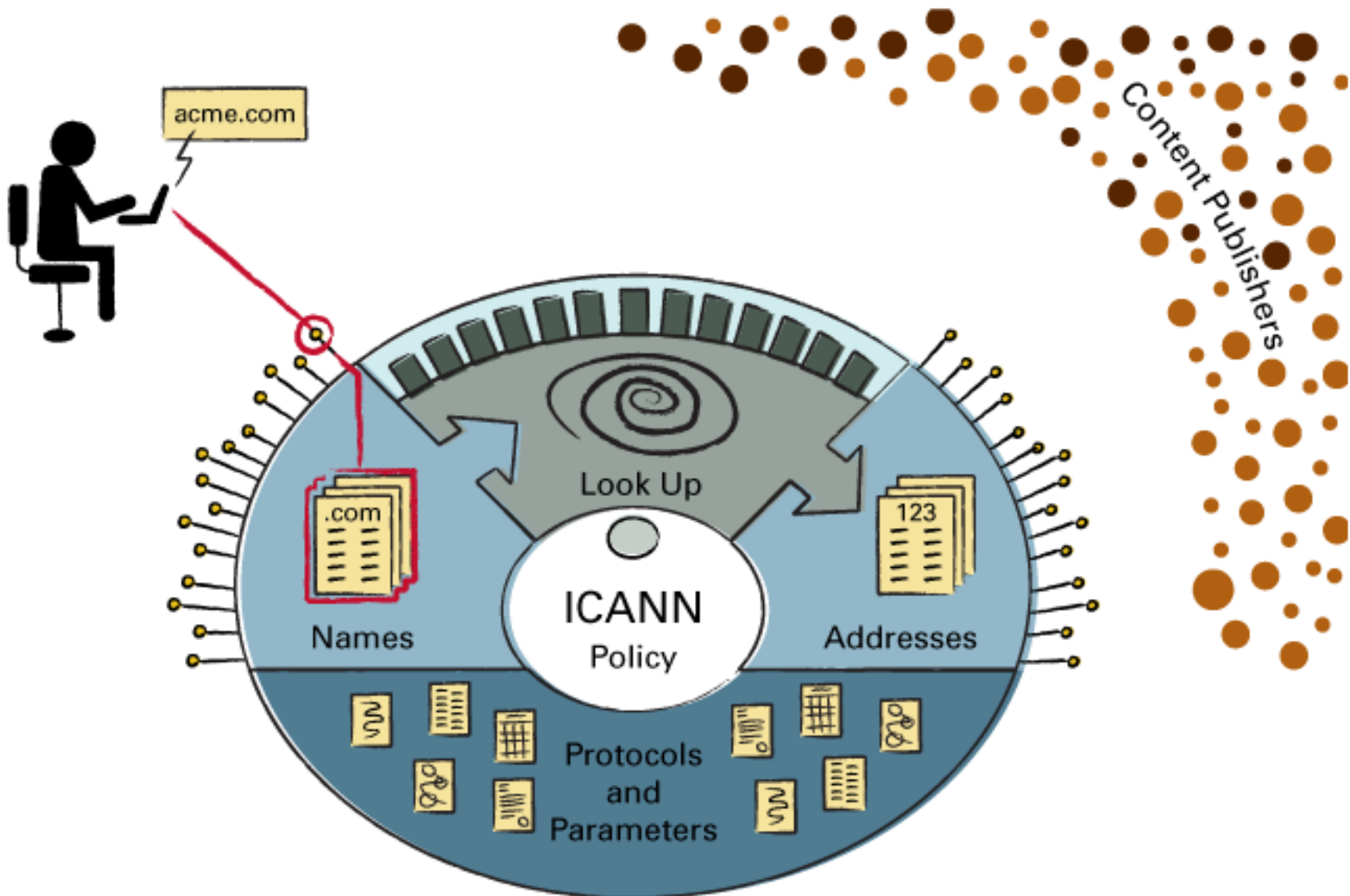
IETF

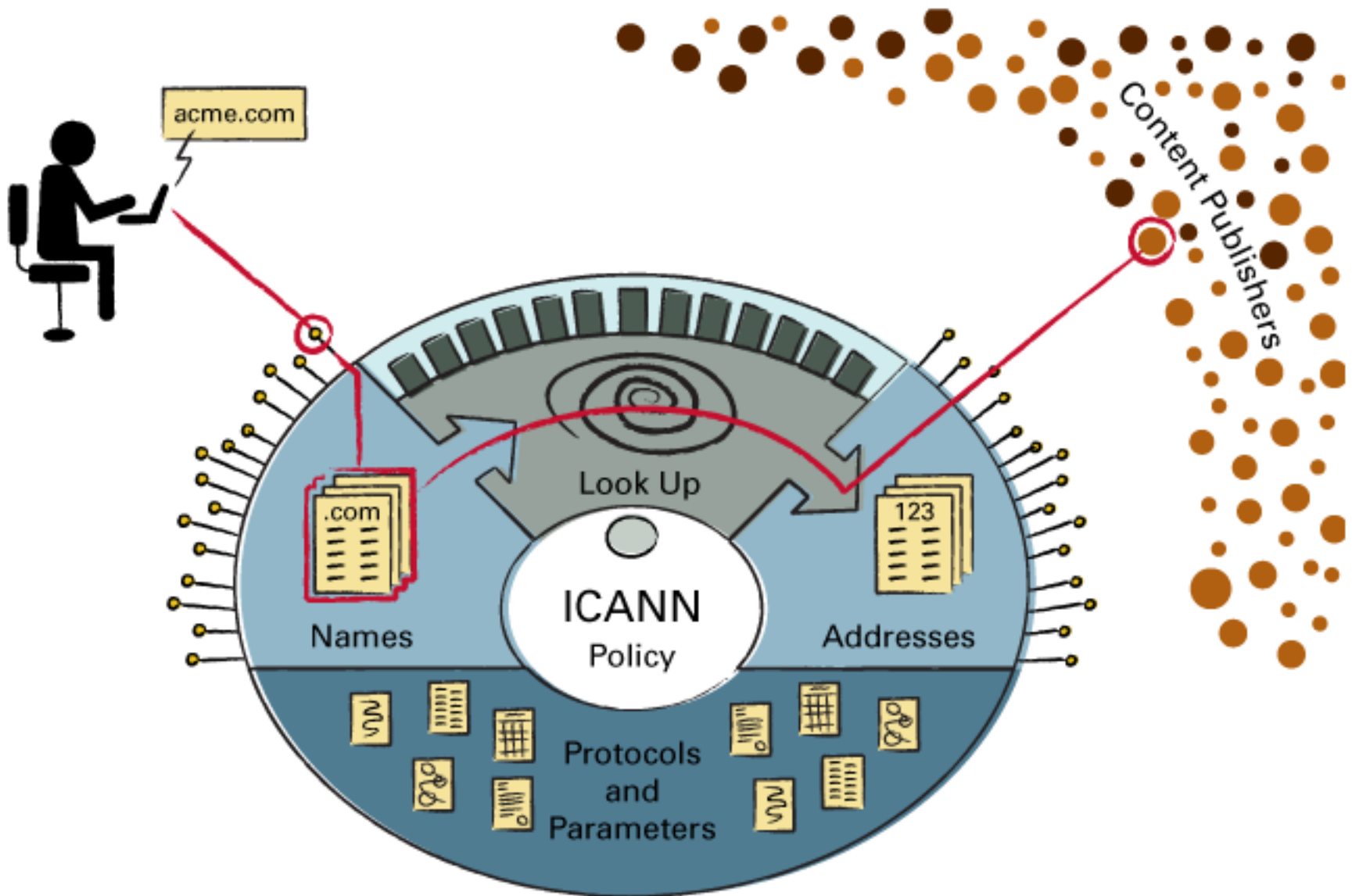


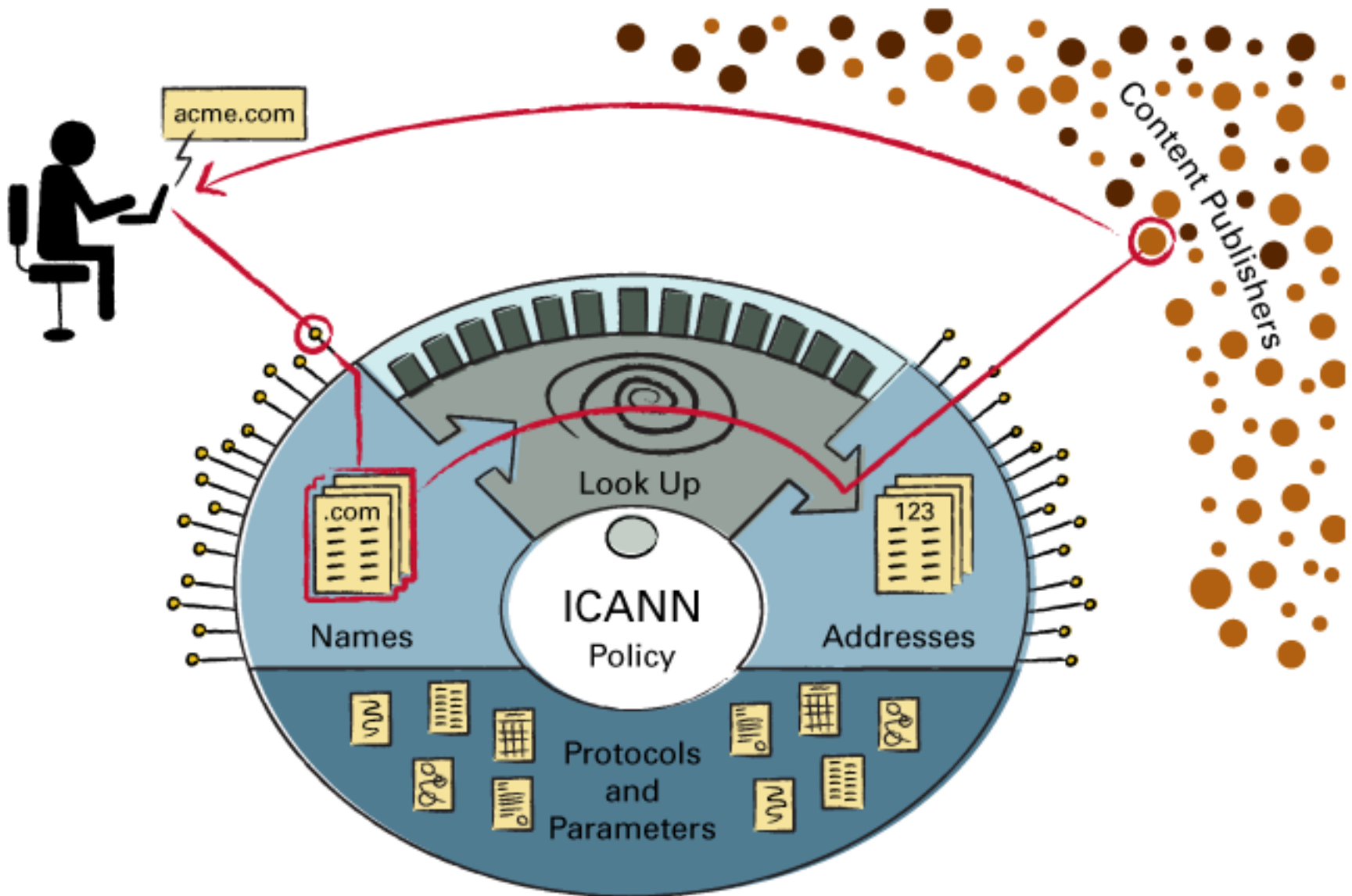


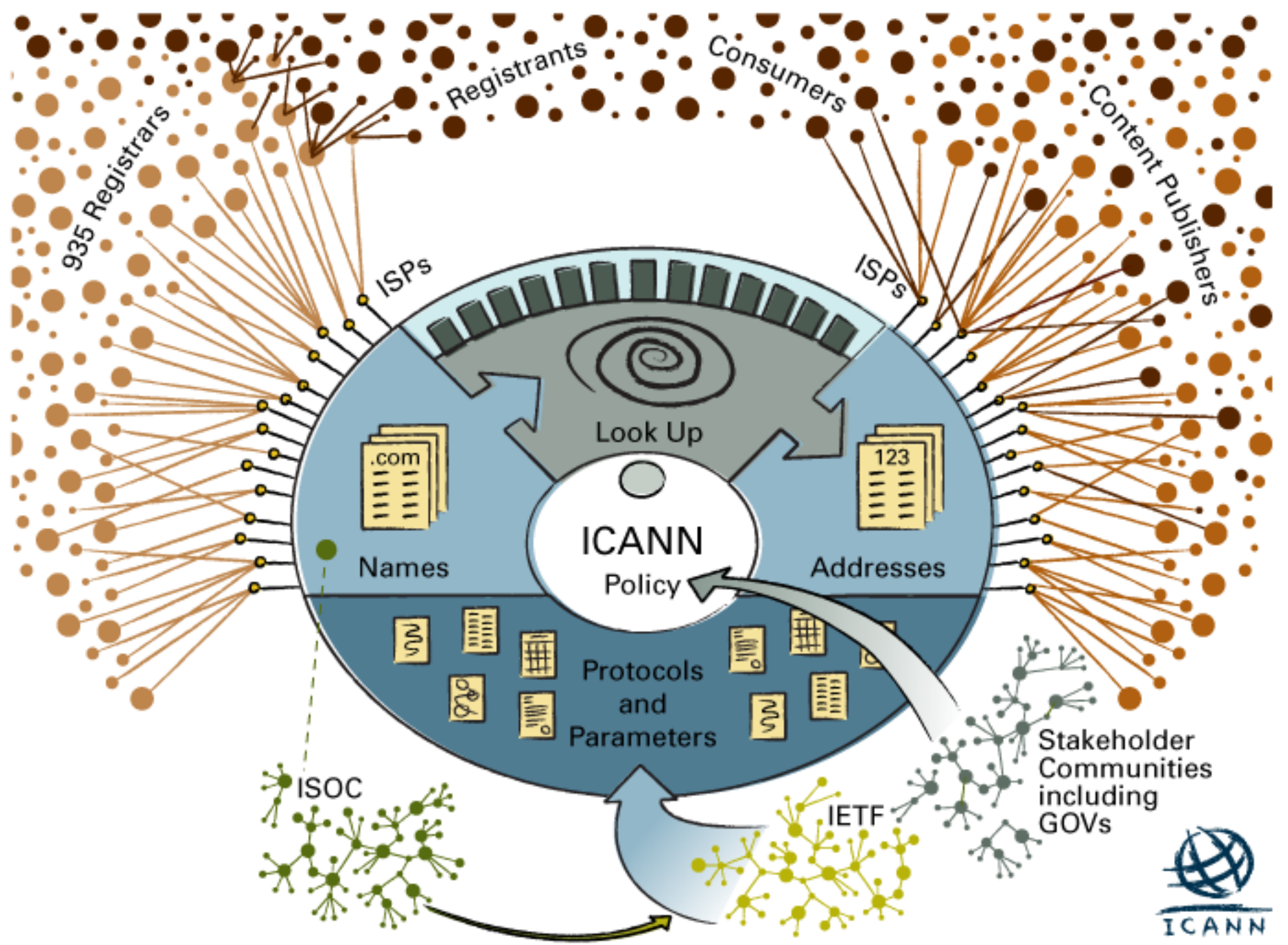












935 Registrars

Registrants

Consumers

Content Publishers

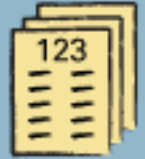
ISPs

ISPs

Look Up



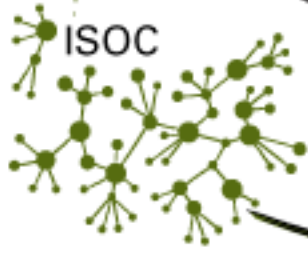
Names



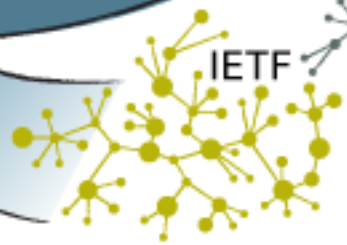
Addresses

ICANN
Policy

Protocols
and
Parameters



ISOC



IETF



Stakeholder
Communities
including
GOVs



DNS: What are the Issues?

- Constantly under attack
- Do we have 100% guarantee that the correct (“intended”) websites are being accessed???
- DNS doesn’t have security mechanisms embedded in it!
- Why? It’s an old system! (30 yrs. old cars too were not built with airbags isn’t it?).

What is DNSSEC?

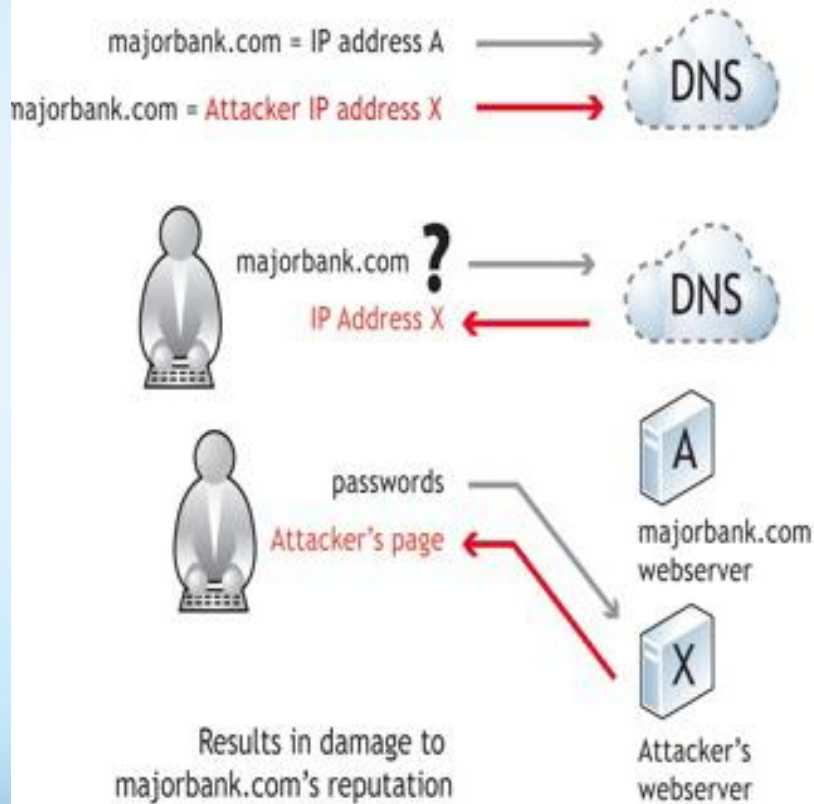
- Internet's phone book (DNS) converts names into numbers, e.g., www.icann.org -192.0.32.7.
- DNSSEC secures the Internet's phone book.
- DNSSEC stands for "DNS Security Extensions."
- Works by incorporating public key cryptography into the DNS hierarchy.
- Is the result of over a decade of community based, open standards development.

What are the DNSSEC benefits?

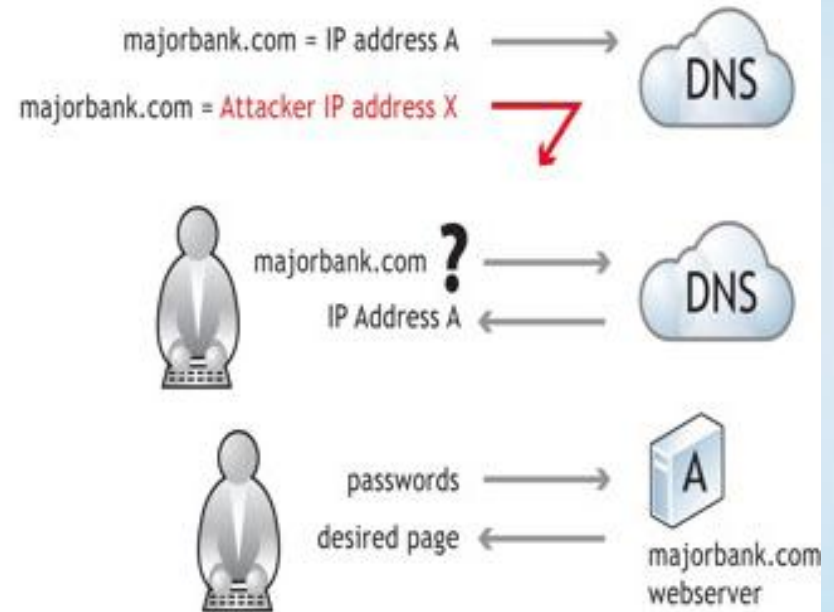
- DNS lookup can be modified in transit to redirect an end user to an impostor or malicious site for password collection (DNS disadv)
- Modification attacks carried out en masse at ISP/enterprise = cache poisoning (DNS disadv)
- A lookup secured with DNSSEC is protected against modification (though not encrypted) = primary benefit.

DNSSEC deployment

Without DNSSEC



With DNSSEC



DNSSEC ccTLD Signing Platform Initiative

- To assist developing nations to be prepared for cyber attacks
- ICANN/PCH collaboration
- No costs involved
- No lock in

Thank you!

shernon.osepa@icann.org