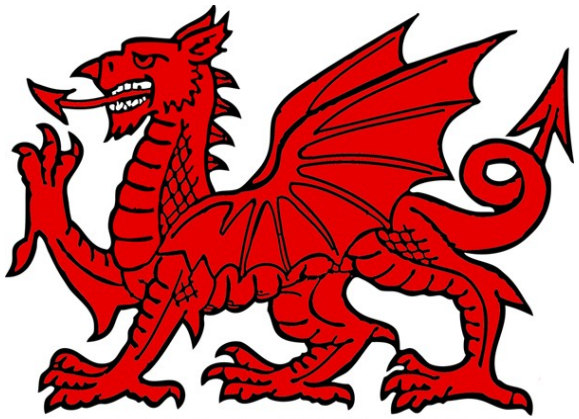
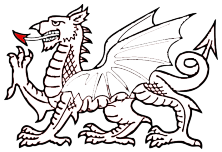
13 Things to Consider Before DNSSEC



John Kristoff jtk@cymru.com

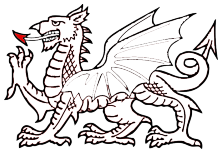
Where is the DNSSEC?

- We make no endorsement of DNSSEC here
- We offer no repudiation of DNSSEC here
- The considerations herein are DNSSEC agnostic
- We argue:
  - From a operational perspective
  - There are 13 DNS questions that must be asked
  - Each answer should be documented



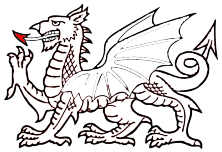
Guidance, not proclamation

- We offer guidance in available choices
- Your posture follows from choices you make
- Your outcome may differ from someone else's
- This may be perfectly reasonable and rational
- Thought is required to make choices intelligently

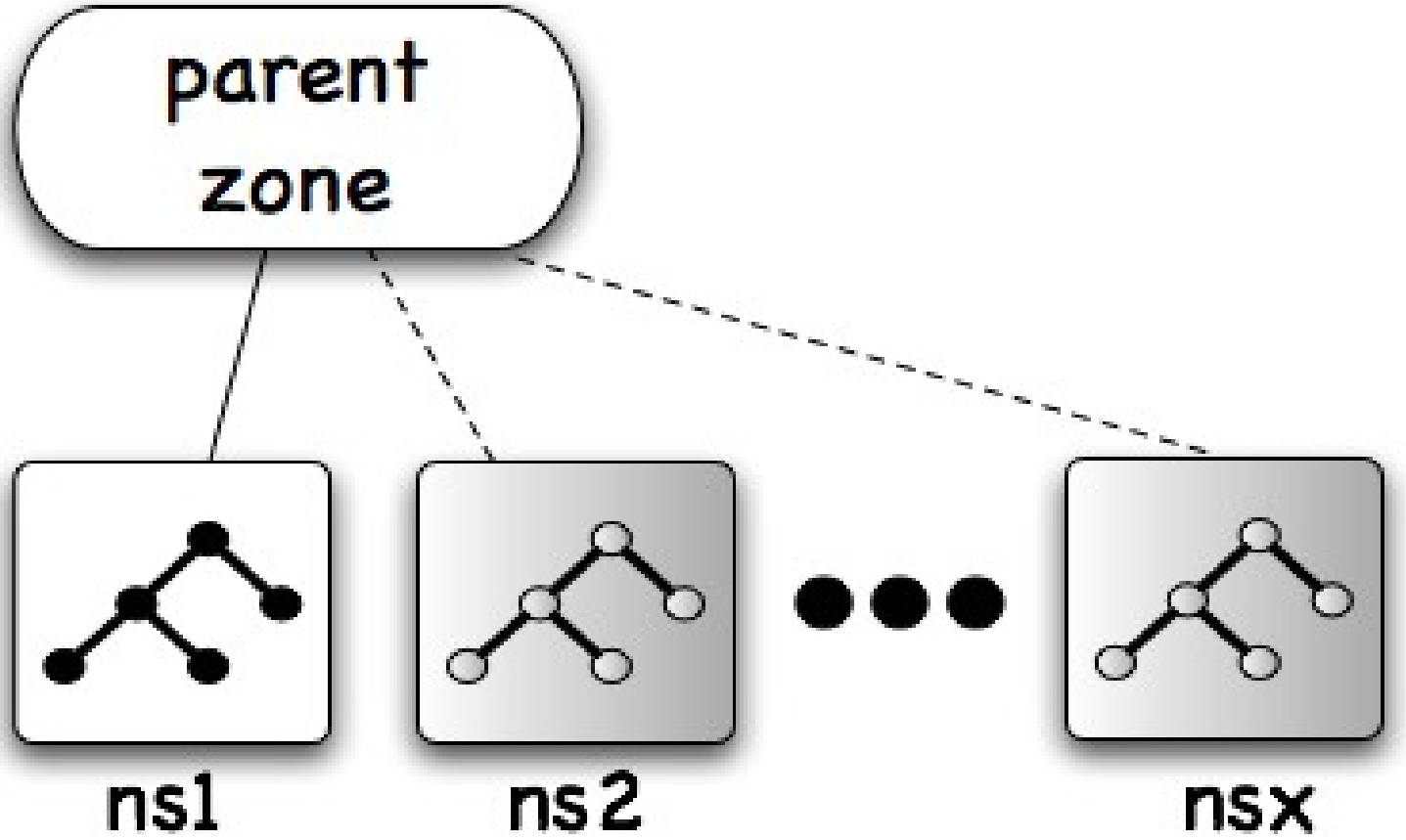


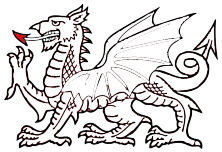
One of two critical systems

Routing (BGP) and naming (DNS) are by far the two most critical subsystems of the Internet infrastructure. And in the case of DNS, practically all Internet hosts participate directly in the DNS as a client, server or both. As a result, DNS is one of the most unencumbered protocols in use throughout the Internet. This can be good, bad or interesting depending on your perspective.



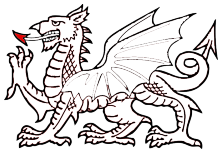
How many NS RRs for your zone?



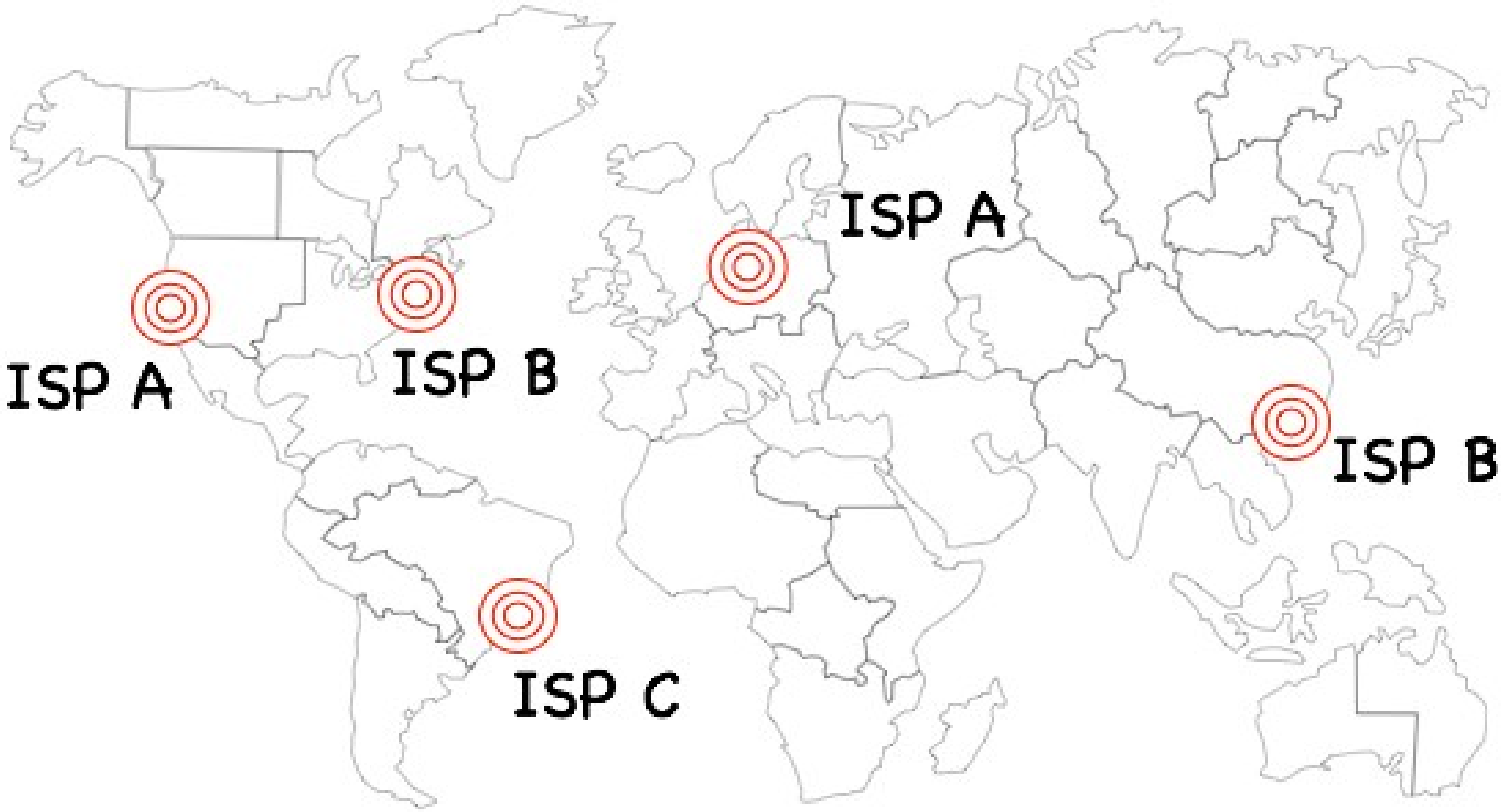


Authoritative name server RRset

- Two is the de facto minimum
- Depending on design, more may be better
- Anycast service may be worth your consideration
- Some people use hardware-based load balancing
- Miscreants invented fast flux
  - Then legitimate providers said, “Hmm...”

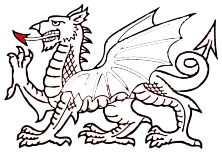


Where are your name servers?

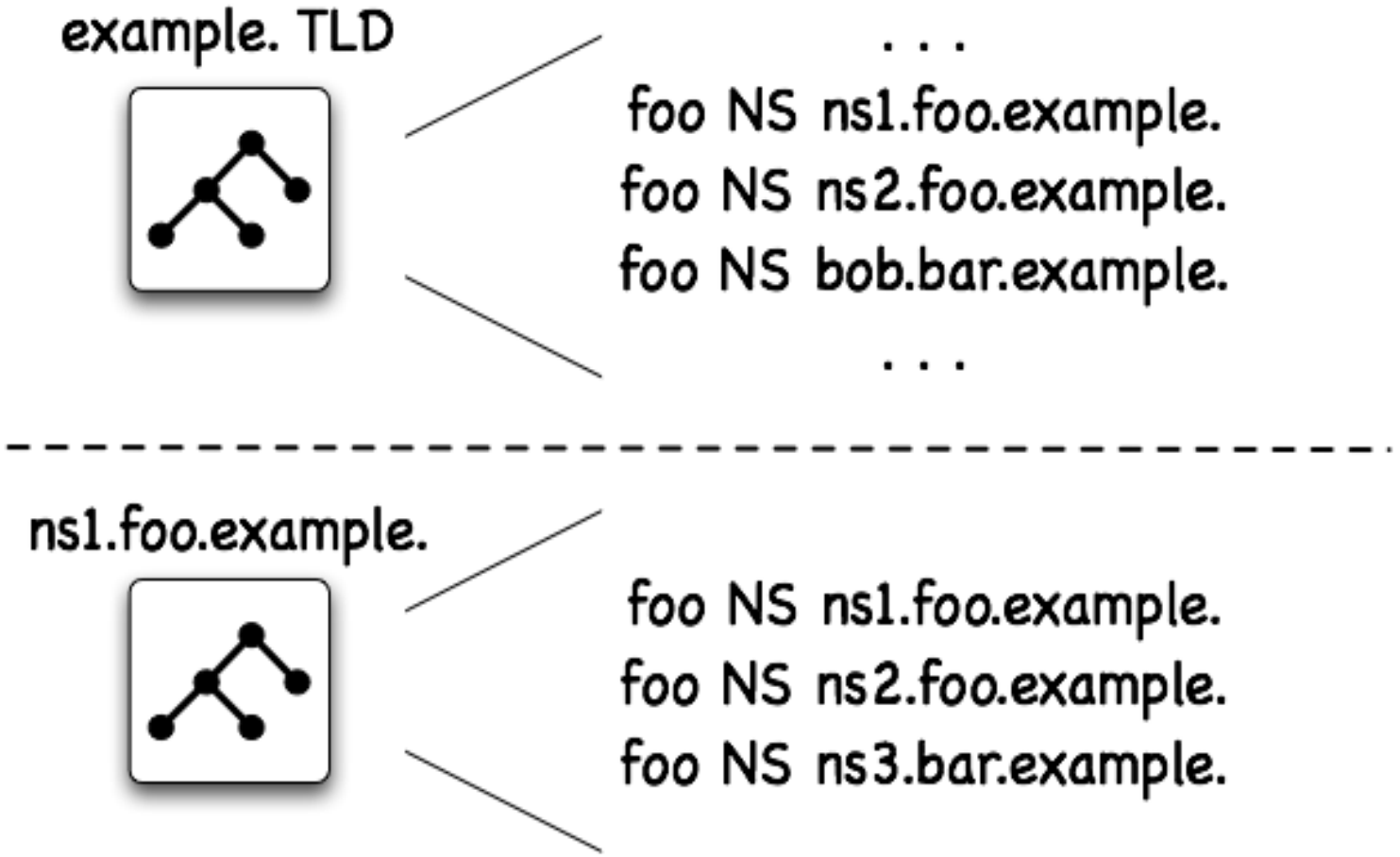


DNS Server Diversity

- Consider physical and topological proximity
- All servers in the same building is suboptimal
  - As are all servers behind a shared upstream link
- Shorter prefixes mitigate route hijacks
- Diverse routing paths can improve resiliency
- Diverse origin AS for routes not strictly necessary
  - Just ask the DNS anycast service providers

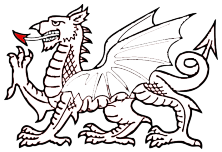


Are parent and children consistent?

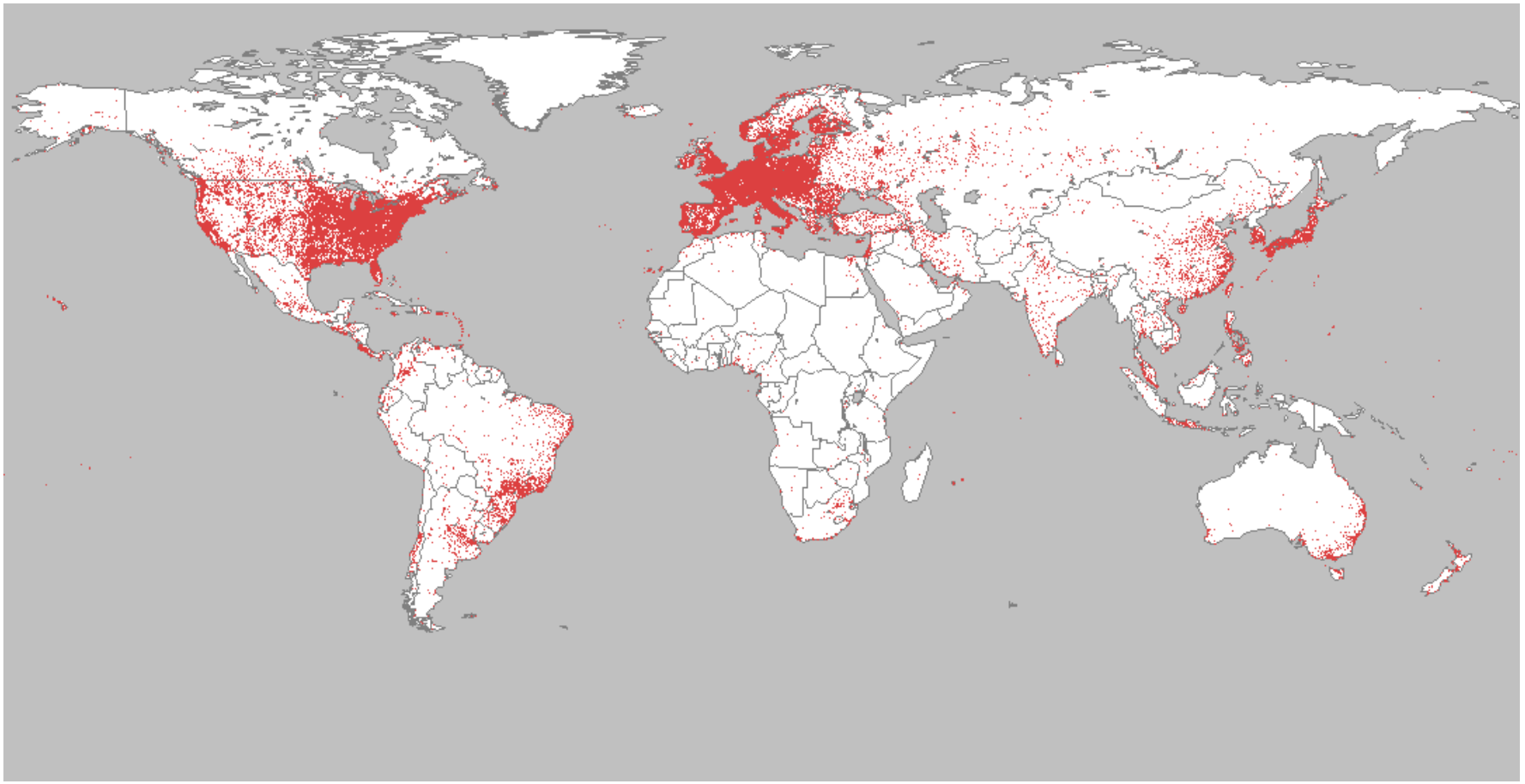


Delegation Consistency

- Things may work if inconsistent, but sub-optimally
  - You're not getting full resiliency at best
  - Delays, timeouts and errors may be occurring
  - Domain name hijacks possible at worst
- Recent measurement showed:
  - 18% of domains in edu. have lame delegations
  - Only 0.1% were REN-ISAC institutions
  - Or less than 5% of all REN-ISAC institutions



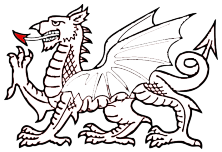
Does your server answer anything from anyone?



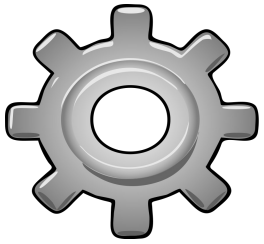
Open Resolvers

- Rarely necessary
- May be used for DDoS reflection and amplification
- Can facilitate cache poisoning attacks
- Can facilitate cache leaks
- We'll tell you about open resolvers on your net:

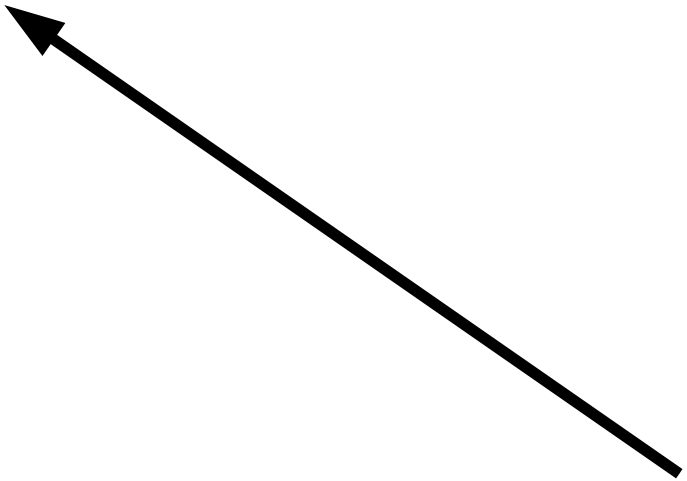
  http://www.team-cymru.org/Services/Resolvers/



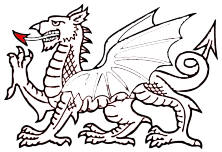
How easily can returning answers be spoofed?



What is the rdata/ttl for ... ?

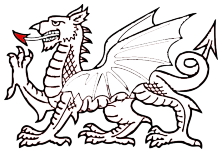


HERE IT IS!! Mmwuahaha...



Answer Spoofing Protection

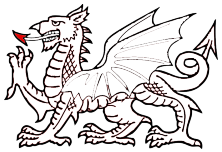
- Implementations need to consider IETF RFC 5452
- Limit recursion (see the open resolvers slide)
- Ideally anti-spoofing is widely deployed
  - See IETF BCP 38 and IETF BCP 84



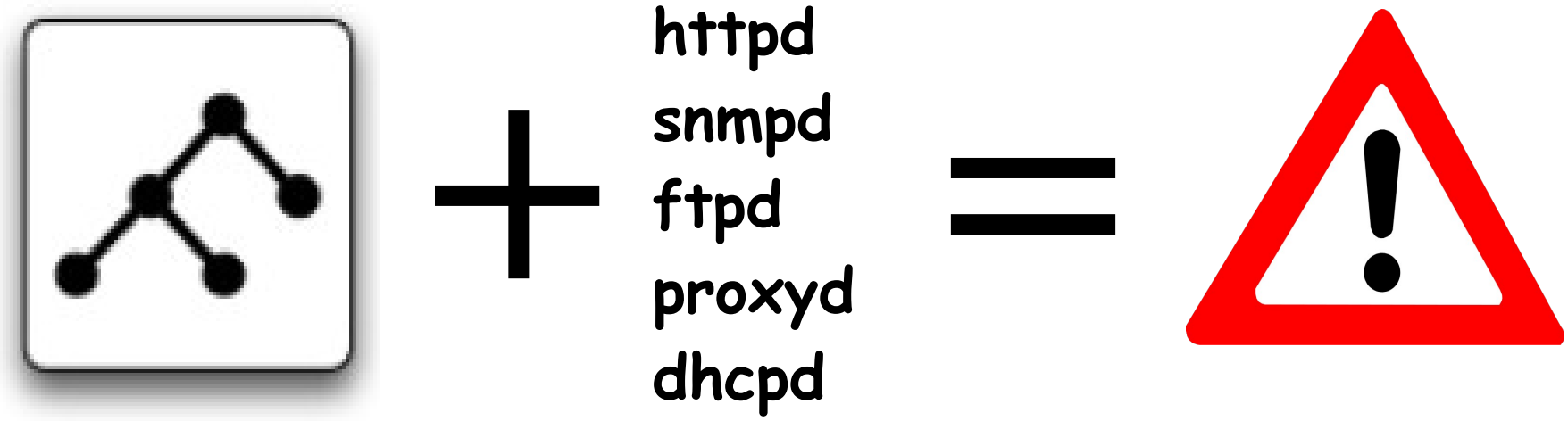
Is your name registration secure?

Domain Name Registration

- Do not let your name(s) expire needlessly
- Safeguard registrar accounts and passwords
- Some registrars offer additional safeguards
  - Ask about them, know what is available
- Make this part of a disaster recovery plan

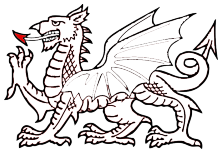


What is on your name server?



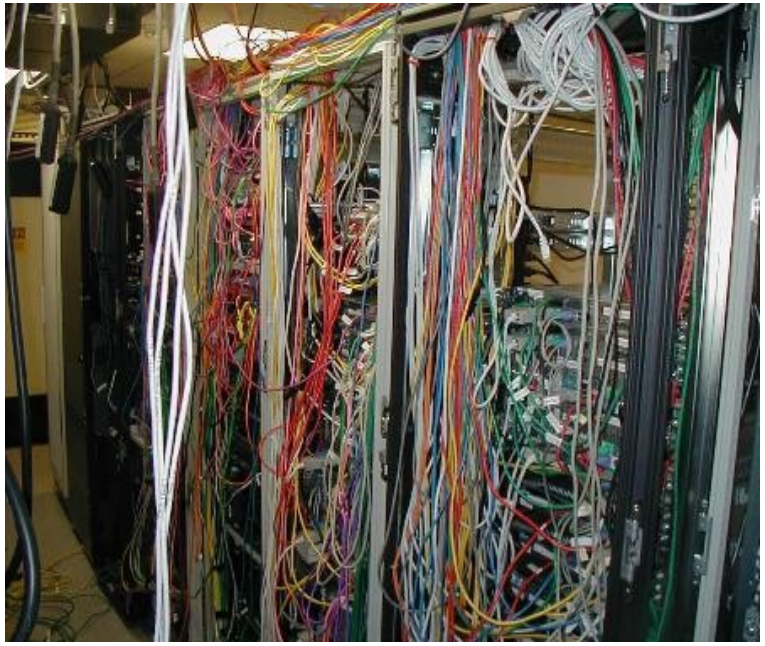
Co-mingling Services

- SSH and NTP are reasonable standard services
  - Most others are not
  - Even these should generally be inaccessible
- Consider isolating some zones from others
  - e.g. put DDoS risk zones on a separate platform



How are servers administered?

pictures from techrepublic, Bill Detwiler

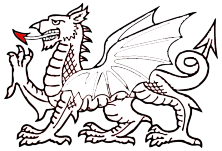


OR

Administrative Processes

- We see a lot of successful SSH brute force attacks
- Limit physical access to facilities and hardware
- If it looks lousy, it probably is
- When in doubt, consult Occam's Razor
- Use revision control for configs and zone files
- As important as a backup plan is the restore plan
- Secure BIND Template

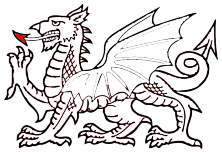
  http://www.team-cymru.org/ReadingRoom/Templates/



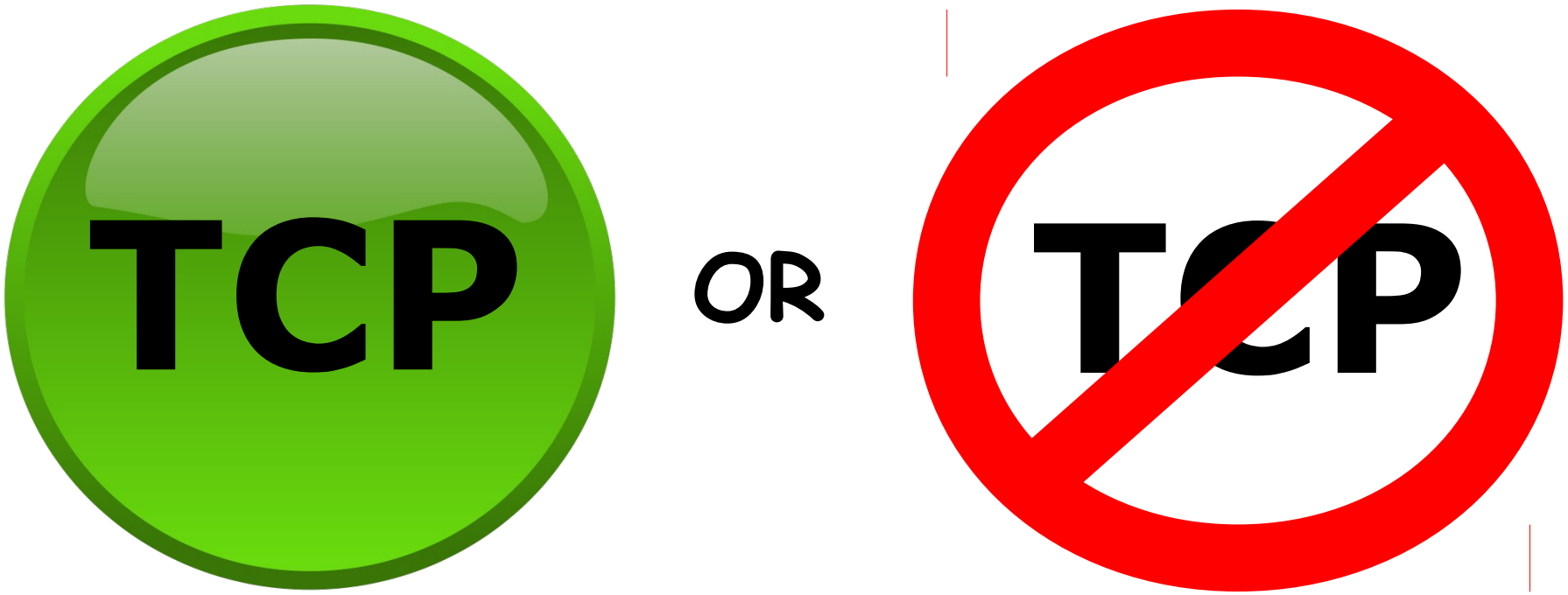
How much RAM, CPU, disk and network capacity is available?

Physical Resources

- Don't have enough, have way more than enough
- Resolvers can demand lots of RAM
- CPU may be important, especially for crypto
- Hard drives usually less important
  - Isolating partitions and directories may be useful
  - Try to offload data collection to another system
- Network capacity usually not an issue until DDoS

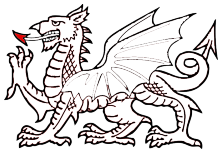


Are you filtering DNS over TCP?



TCP

- Don't assume you have no DNS over TCP
- TCP isn't just for zone transfers
  - Large DNS messages may use TCP
  - Some operators may force TCP during DdoS
- TCP tuning may be required for some DoS threats



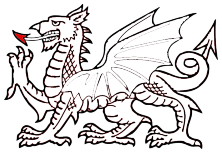
What queries do you see/make?

Monitoring and Auditing

- Troubleshooting with query insight is very helpful
- Consider learning answers from your resolvers too
  - AKA passive DNS
- Minimally, trend DNS query/answer statistics
- Monitor servers, answers and routes from outside

  http://www.team-cymru.org/Monitoring/DNS/

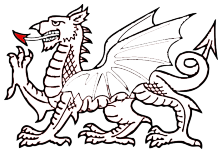
  http://www.team-cymru.org/Monitoring/BGP/



Are name server clocks accurate?

Time Synchronization

- This probably means running NTP properly
- Troubleshooting works best with good timestamps
- Collected data is practically useless if time is off
- Some protocols require coordinated time
  - e.g. TSIG
- Consider setting clocks to UTC
  - Helpful for correlation across timezones

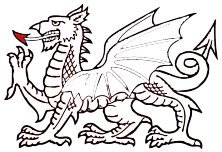


Have you read IETF RFC 2870?

Network Working Group
Request for Comments: 2870
Obsoletes: 2010
BCP: 40
Category: Best Current Practice

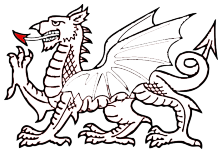
R. Bush
Verio
D. Karrenberg
RIPE NCC
M. Kosters
Network Solutions
R. Plzak
SAIC
June 2000

Root Name Server Operational Requirements



IETF RFC 2870

- Its a BCP, you should be familiar with it
- Its a bit dated and written for a specific audience
  - But it contains sound advice for most everyone
- A newer, generalized version may soon appear



How can Team Cymru help?

- Secure BIND template
- Open resolver feed
- DNS and BGP monitoring
- Returning soon: Lame delegation report
- Coming soon: Netnames
- Coming soon: DNS Report
- Preso feedback or questions to: jtk@cymru.com
- Everything else is @ http://www.team-cymru.org