DNS-SD Hybrid Proxy
NANOG 61

June 2014

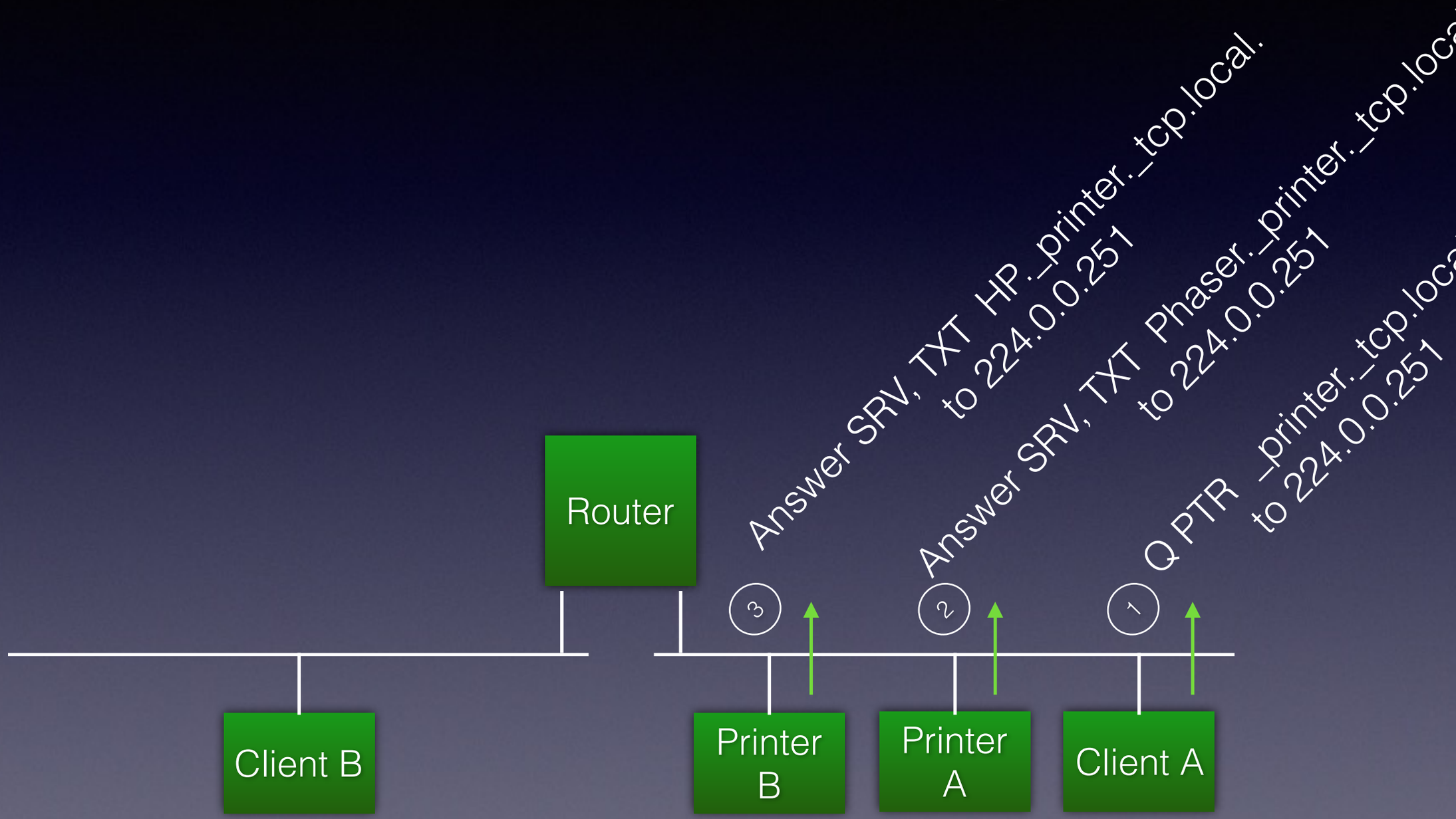
Tom Pusateri <pusateri@bangj.com>

Updated: 6/4/14

mDNS Service Discovery

- Services are described by service.proto.domain.
    - Example: _printer._tcp.local.
- Query PTR resource record to find instances
- Answers are PTR instances and SRV, TXT resource record pairs
    - _printer._tcp.local. PTR Phaser 6180._printer._tcp.local.
    - Phaser 6180._printer._tcp.local. SRV 0 0 631 color-laser.local.
    - Phaser 6180._printer._tcp.local. TXT “Color=T Duplex=T Scan=N”
- Answers are instance.service.proto.domain
- .local domain represents link-local services not requiring unicast DNS
- queries/answers sent to link-local IP multicast group 224.0.0.251 / ff02::b

mDNS Example



mDNS Limitations

- Link-local - doesn’t work across campus
- IP multicasts wake up all Wi-Fi (mobile) devices
- No current mechanism to filter services on L2
- Next attempt: Wide-Area Bonjour

Wide-Area Bonjour

- 1st attempt to share services across campus
- unicast DNS server becomes aware of services through SRV, TXT, & PTR resource records
- clients dynamically update unicast DNS with services they want to advertise
- or administrators statically configure services
- clients then search unicast DNS domain:
  - Query PTR _ipp._tcp.example.com.

Wide-Area Bonjour Limitations

- administrators don't want dynamic updates to their unicast DNS servers
- could create subdomain (dyn.example.com) but disseminating security credentials a problem
- static entries are difficult to capture and enter
- static entries get stale and new services not added

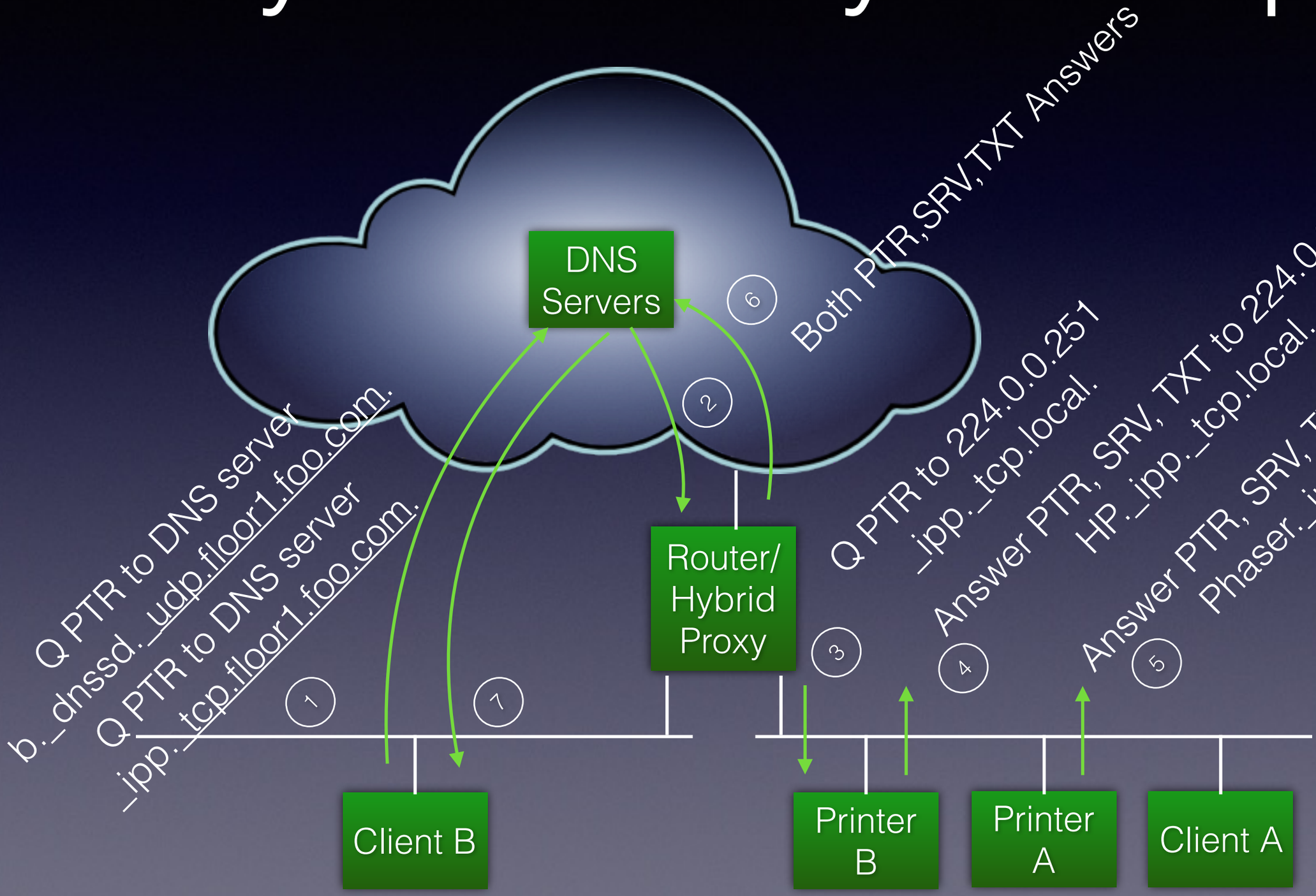
Educause Petition

- Universities collectively petitioned Apple for help
  - Enhance bonjour to work across IP subnets
  - Enhance Apple TVs to work across IP subnets
    - Add WPA2 Enterprise authentication to Apple TV
- IETF joined and formed DNSSD working group
  - requirements defined but no solution selected yet
- Apple proposes the DNS-SD Hybrid Proxy to extend bonjour
  - http://tools.ietf.org/html/draft-cheshire-dnssd-hybrid-01

DNS Service Discovery Hybrid Proxy

- dynamically map between mDNS & unicast DNS
- each .local subnet has a unique subdomain
- subdomain delegated to hybrid proxy attached to subnet
- inside subnet, mDNS works as usual
- outside subnet, .local mapped to subdomain.example.net
- subdomain then added to clients DNS search domains
- unaware, unmodified clients search like wide-area bonjour
- hybrid proxy could be in router, switch, or stand alone server or vm

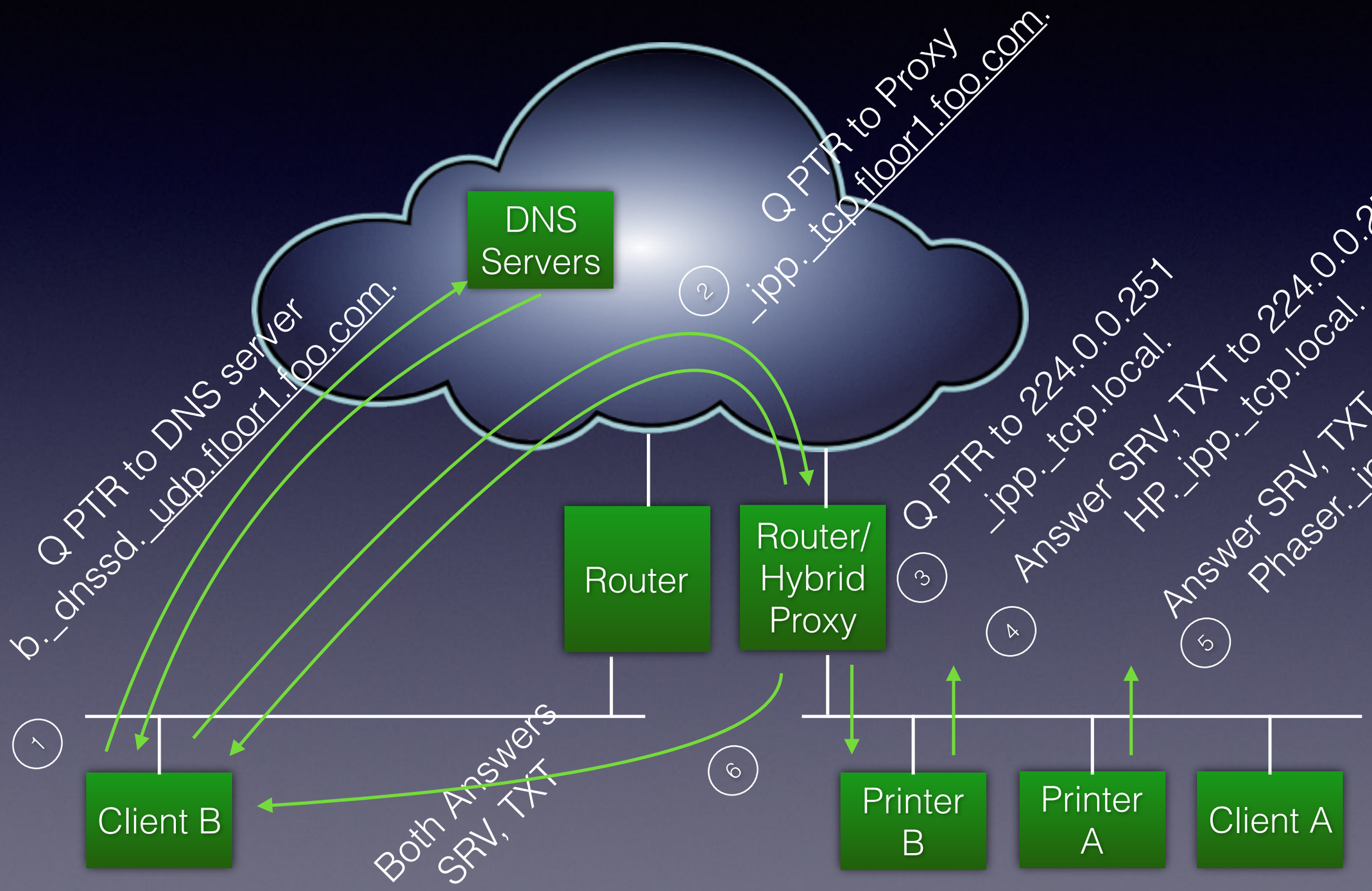
Hybrid Proxy Example



Long-Lived Queries (LLQ)

- Discovering new services or dropping stale services via unicast requires constant polling
- pub/sub extension allows client to express interest in service type and receive constant updates
- EDNS(0) option is used to subscribe & publish changes
- first used with wide-area bonjour
- implemented in clients but not many servers
- adopted by Hybrid Proxy to alleviate polling & to direct queries to proxy for potential policy decisions
- alternate pub/sub methods also being considered for hybrid proxy

Hybrid LLQ Example



Hybrid Proxy Limitations

- Without LLQ, query source isn't available for policy
- link-local IP addresses must be suppressed
- cache might not be complete for unicast queries
- answer aggregation can produce large DNS packets
- existing clients will combine services into flat list
- lots of potential subdomains in DNS search space
- NSEC translation difficult due to incomplete knowledge

Implementation Status

- OpenWRT by Markus Stenberg
  - https://github.com/sbyx/ohybridproxy
- hypd by Tom Pusateri
  - commercial version runs on any BSD/Linux
  - Downloads available soon at http://hypd.info
  - meant to be embedded in routers/switches/APs