How IPv6 and DNSSEC change the Intranets

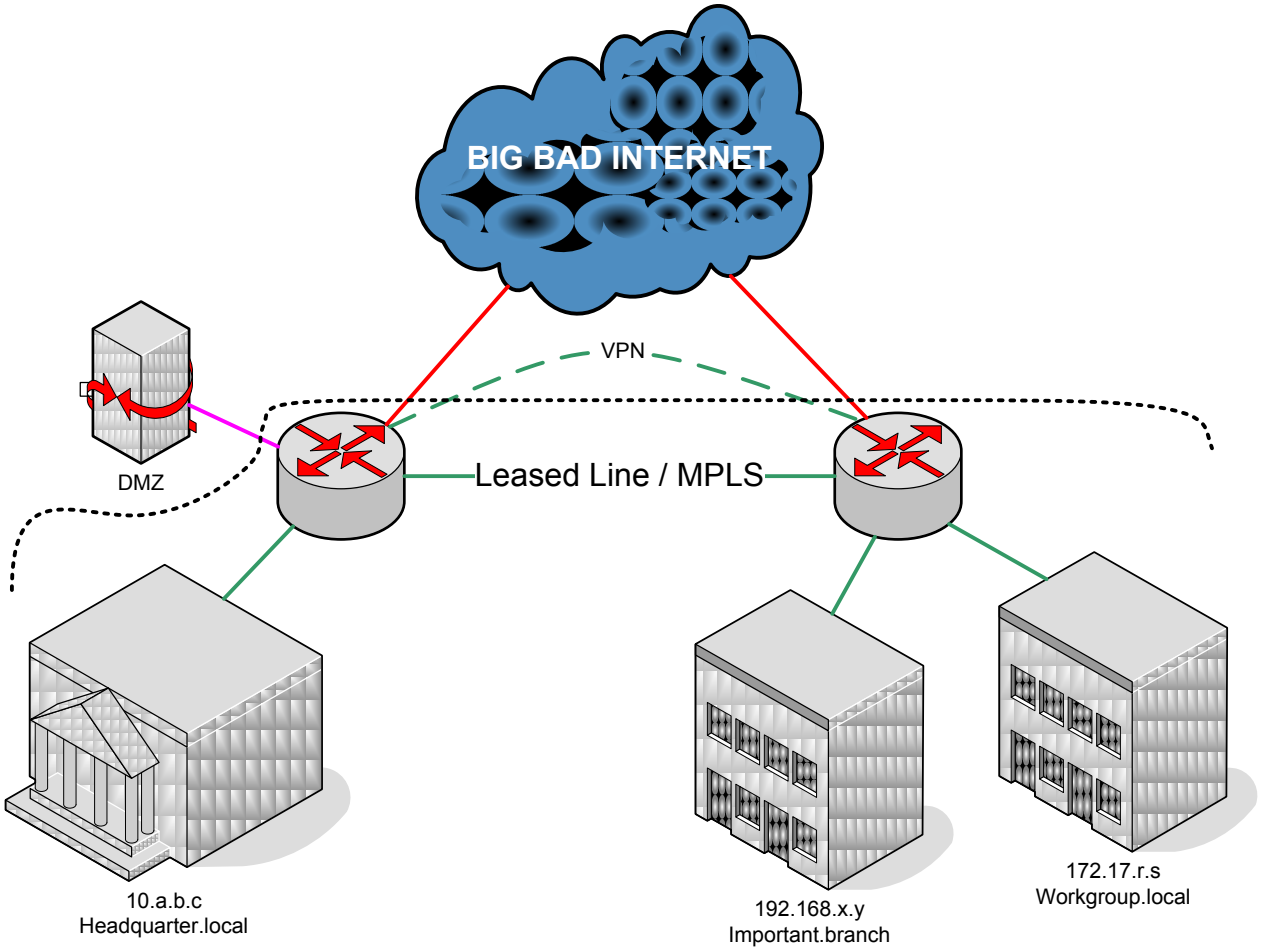
Lutz Donnerhacke
lutz@iks-jena.de
OpenPGP db089309
1c1c6311ef09d819 e02965bebfb6c9cb

ICANN

Current practice

- Build a separate network using site specific names and numbers
- Provide application layer gateways, NAT, Split-DNS, and VPN for non-local access
- Hide internal structure
- Statically map necessary services
- Provide local “root” services

Current practice example



The IPv6 impact

- IPv6 provides **public**, globally routable IPs
  - Clients do IPv6 automatically (even tunnel)
- IPv6 provides **end-to-end** communication
- IPv6 is *not* designed to be *translated*
- Future protocols rely on **direct** channels
  - Web 2.0: Numerous bits from different servers
  - Client to client communication
  - Shortest routing for “quality enhancements”

The DNSSEC impact

- Validation chain from a **well-known key**
  - Clients may have the key hardcoded
- Only **one root** possible
  - *No local* names
- Prevents rdata and NXDOMAIN rewriting
  - **Consistent** external and internal view
- Enterprise DNS rely on DNSSEC from everywhere (DirectAccess, SSH, _tcp …)

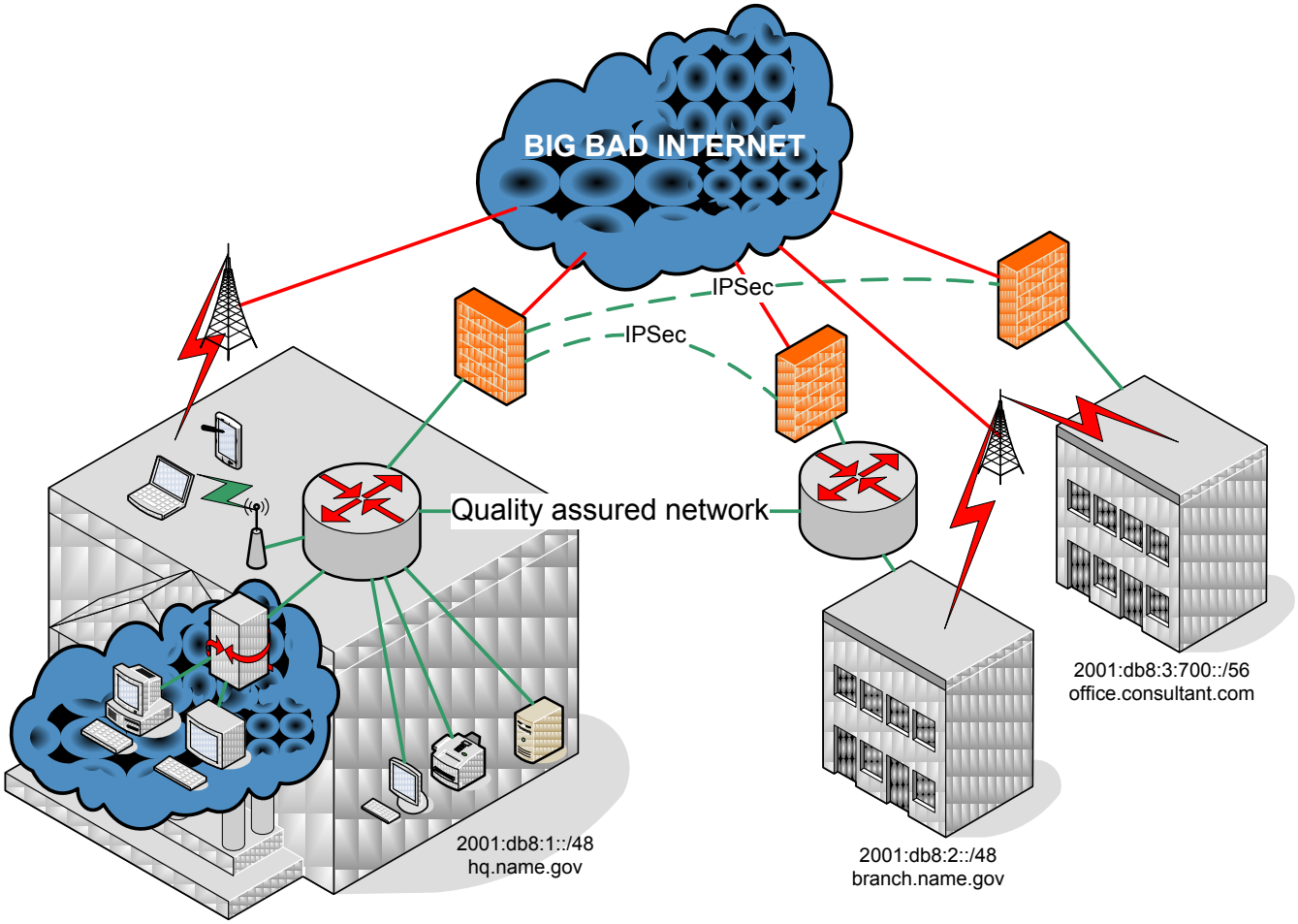
The horrible mobile client

- Public mobile networks are everywhere
- Mobile clients
  - Important status symbols
  - Roam in and out quickly
  - Always on: Cloud services
  - **Can’t be configured**
- IPv6
  - Exposes internal DNS servers
  - Create mobile peer-to-peer networks

First approaches

- Filter packets, not hiding addresses
- Transparently tunneling insecure nets
- Use routing to keep domains and quality
- Surviving legacy addresses
  - Keep *NAT*, because the pool is empty
  - Signed *Split-DNS* with **two** DS records
  - Find and *replace* legacy hardware
  - *Encapsulate* legacy IP in **to-be-removed** nets

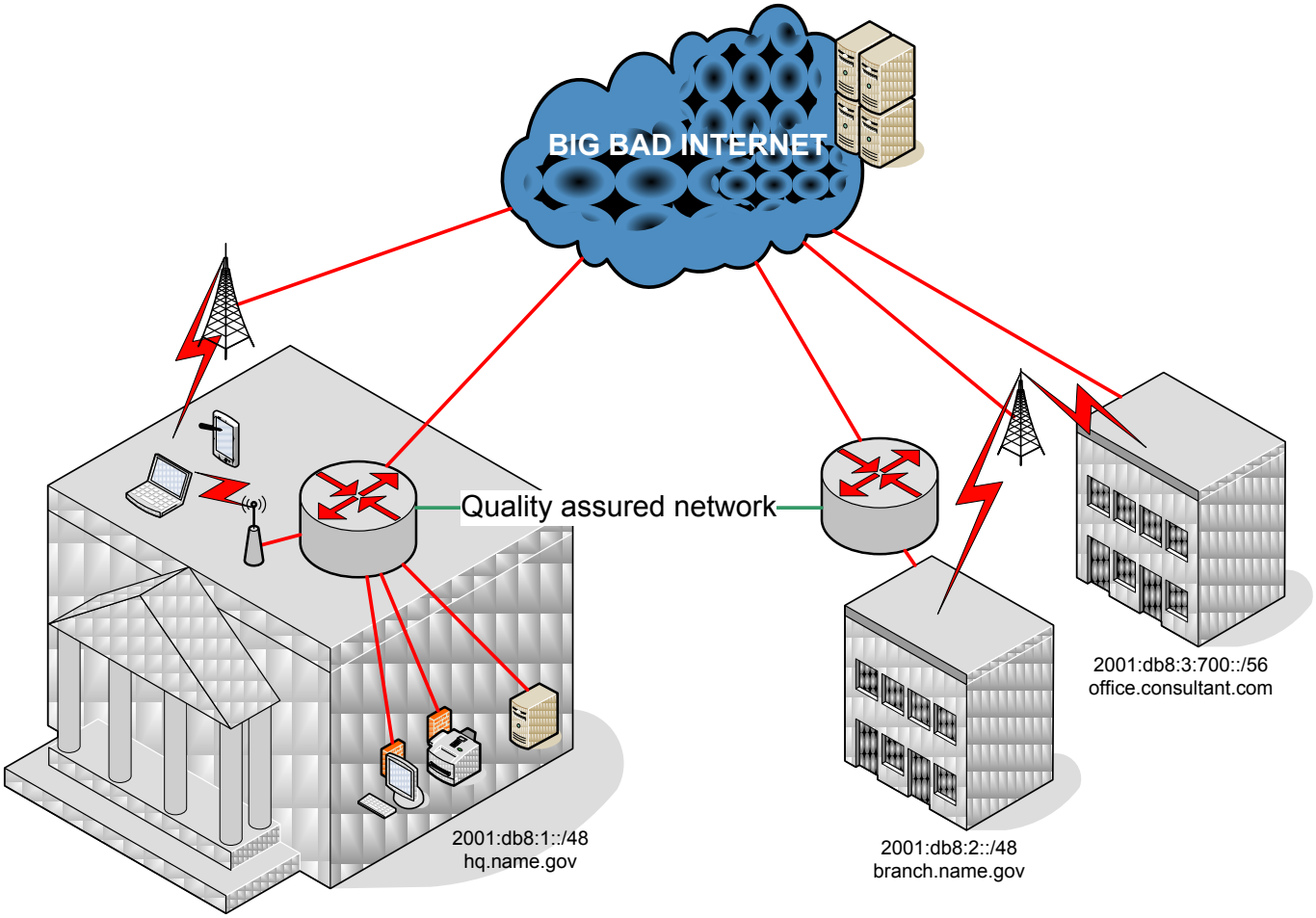
Intermediate example



Modern intranets

- **Accept** consistency requirement
  - Local WLAN *and* mobile networks
  - REST web applications instead of VPN
- Secure the services, not the networks
- Secure the data, not the servers (cloud)
- Authenticate the user, not the computer
- Use DNS as trustworthy resource
- Always use direct communication

Modern Intranet



Conclusion

- IPv6 and DNSSEC dramatically change the design of modern networks
  - Information hiding policies do not work
  - Centralized policy enforcement unusable
- Concentrate on benefits
  - Build stable, globally routable networks
  - Enforce data security at the data level
  - Trust the people, not the devices

Questions?

Lutz Donnerhacke
lutz@iks-jena.de
OpenPGP db089309
1c1c6311ef09d819 e02965bebfb6c9cb

ICANN