Worst Current Practice

Lutz Donnerhacke
IKS GmbH
Worst Current Practice

• Not a talk about “simple” bugs
  – Too many WTFs to talk about
  – Sometimes instructive anyway
    • SEOS: IPv6 packets crash Ether Channels: Card reload
    • SEOS: Loopback take status from management interface
    • nPA software not for Solaris, NeXT STEP or VMS
  – Worst case reaction: Documentation bug
  – Typically caused by too limited testing facilities
    • Solution: Urge your suppliers to include your case!
Worst Current Practice

- Talking about network design choices
  - Based on reasonable (but wrong) assumptions
    - You can’t throw away the concept at meetings
  - Requires manual corrections at unrelated places
    - Extensive recovery procedure handbooks
  - Long term job security
    - Experience necessary to maintain the network

The way to hell is paved with good intentions
IPv6 addressing

- ipv6 address autoconfig set-route
  - Centralized infrastructure
  - Self healing
- ipv6 address 2001:db8::/64 eui64
  - Copy and paste
  - Unique addresses
- ipv6 address 2001:db8::169:254:1:3/64
  - Common identifiers for each family
- ipv6 address 2001:db8::1/64
  - Usage based addressing
IPv6 addressing

- ipv6 address autoconfig set-route
- ipv6 address 2001:db8::/64 eui64
  - Address changes at hardware exchange or reboot
  - Manually configured routes need to be changed
- ipv6 address 2001:db8::169:254:1:3/64
  - EUI64 requires special handling of the two MSBs
  - Renumbering causes double headache
- ipv6 address 2001:db8::1/64
  - Hard to add a second device
IPv6 addressing

• Windows 2008R2 and beyond
  – Set an unique identifier at initial setup
  – Add a fixed offset per interface
  – Survives hardware change and extension

• Privacy extensions and reverse DNS
  – Clients should update DNS (daemon easy to write)
  – Monitor router log files to update DNS

• Firewall “enforce EUI64”: bad choice
  – Checks for ...ff:fe...  WTF?
Simple DNS errors

$ dig ds com @8.8.8.8 +dnssec +nottl +nocl

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20249
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;com. IN DS

;; AUTHORITY SECTION:
com. SOA a.gtld-servers.net. nstld.verisign-grs.com. 1288863778 1800 900 604800 86400
Simple DNS errors

• Google claims Public DNS supports DNSSEC
  – Service does not handle DS correctly
  – Fundamental software design bug
  – Internal data structures are insufficient

• Result of this “bug”
  – www.google.com is an alias for www.l.google.com. (BOGUS (security failure))
  – www.l.google.com has IPv6 address 2a00:1450:8007::6a (BOGUS (security failure))
  – Reason: no DNSSEC records from 8.8.4.4 for DS com. while building chain of trust

• Google can’t resolve www.google.com
  – http://wwwneu.iks-jena.de/ger/Tools/DNSSEC/Pruefen
Windows basics

• DNS servers assigned to interfaces
  – Single use to *update* the DNS in each network
  – Ask all servers on all interfaces to *resolve* DNS
  – Stay on the *fastest* server until errors
  – DNSSEC for remote access, required by DirectAccess

• VPN
  – adds an new extra interface
  – modifies routing table
  – Host route to VPN peer to “old” default gateway
  – Optional new default route with metric to VPN peer
VPN into Windows network

- All AD discovery procedures use _TCP.do.main
- VPN fails constantly in China or via DTAG
  - DNS server (CPE) reachable despite VPN
  - NXDOMAIN rewriting gives wrong results
  - Join to AD via VPN fails

- Solutions
  1. Internal DNS reachable via public DNS resolution
  2. route add <cpe-gw> via <vpn-gw>
  3. Block external DNS traffic at VPN gateway
Advanced DNS errors

• Microsoft DPM for Backup
  – Huge data can cause congestion
  – Backup data is sensible
  – Separate infrastructure recommended

• How DPM works
  – Lookup IP of DPM server via DNS
  – Connect to DPM, transfer data
  – Transfer Snapshots

• DPM does not accept non-AD clients (or so)
Advanced DNS errors

- **Failover in DPM**
  - All devices update DNS regularly on all interfaces
  - Microsoft DNS expires dynamic updates
  - Microsoft DNS avoids round robin in this zone
  - Applications use first entry first
  - DPM server has an network priority override

- **DPM connects to the “secondary” address**

- **On failure, the entry times out: other net used**
Ignore Lifetimes

- Common error
- Application takes DNS result as forever
  - Reboot regularly
- Firewalls use DNS results forever
  - Manual update on customer demand
- iPhone takes DHCP result forever
  - Lease never renewed
  - Assumption: User leaves before lease expires
Questions?

Lutz Donnerhacke

dig NAPTR 1.6.5.3.7.5.1.4.6.3.9.4.e164.arpa. +dnssec

OpenPGP: DB089309 lutz@iks-jena.de
1C 1C 63 11 EF 09 D8 19 E0 29 65 BE BF B6 C9 CB