DNS and DHCP
Contents

• Introduction
• DNS at the University of Reading
• DHCP myths
• DHCP at the University of Reading
Introduction

- DNS: Domain Name Service
  - Global Internet service
  - 114 RFC documents on DNS
  - In simplest form provides name to IP address and IP address to name lookups
  - More complex deployments also use DNS for locating services, looking up telephone numbers, providing anti-spam measures, etc.
  - Arranged as a tree, split into ‘zones’
  - Each zone can be delegated to a different authority
  - Forward and reverse zones
  - Concept of ‘resource records’ (RRs)
    - A, PTR, NS, MX, SRV, TXT, AAAA, etc.
Introduction

- **DHCP: Dynamic Host Configuration Protocol**
  - As name suggests, provides network configuration information to hosts, on request
  - Most common deployments use DHCP to configure:
    - IP address / subnet mask / default gateway
    - DNS server IP address(es) / domain name
  - Microsoft-friendly deployments also configure:
    - WINS servers
    - Netbios node type
  - But can also be used for a whole lot more:
    - Boot server IP address and file name
    - Configuration files for printers / IP phones
    - Pretty much anything else, through Vendor-Specific Options (option 43)
DNS at UoR

- IT Services is the naming authority for UoR
  - Nominated contact for JANET and other registrars
  - Operate and maintain DNS servers
  - Define hostname policy but reasonably flexible on aliases
  - It has to be this way or end up with anarchy

- Over 50 zones
  - Try to avoid subzones of rdg.ac.uk and reading.ac.uk if possible
  - rdg.ac.uk ≠ reading.ac.uk
  - Some zones only resolve internally, i.e. are not Internet-facing
    - Used for internal-only services and infrastructure
    - private.rdg.ac.uk and private.reading.ac.uk
DNS at UoR

- Server infrastructure currently consists of:
  - Nine Infoblox Appliances
    - Two for management
    - Three for external-facing DNS
      - Two at UoR, one at Greenlands
    - Two for internal-facing, recursive DNS
      - Allow non-authoritative lookups on behalf of clients
    - Two for DHCP
      - Two Sun Fire V210 servers
        - To be retired in 2009
      - One Linux virtual machine
        - Internal-facing DNS at Greenlands campus
DNS at UoR

- All servers authoritative for our zones
  - Updates happen within 10 seconds internally
  - But can take up to 24 hours to propagate across the Internet
    - Depends on time-to-live (TTL) of the RR being changed
    - So to be certain:
      - Allow 24 hours for updates
      - Or plan ahead and ask for the TTL to be lowered
  - Key services have TTL set to 5 minutes
    - www, email, vpn, blackboard
  - Low TTL facilitates more rapid disaster recovery
    - But causes higher load on authoritative DNS servers
DNS at UoR

• IT Services will:
  – Allocate hostnames and IP addresses for your devices
  – Allow any reasonable, non-offensive alias(es) for a device
    • Some aliases are reserved for IT Services use
      – Typically Internet service names, such as www, dns, ldap, mailhost, proxy, news, etc.
      – But we can create special ones for you – ldap.sse
  • But reverse-resolution will be to the allocated hostname
    – Unless there is a good technical reason not to

• IT Services will not:
  – Allocate wildcard records unless there is an incredibly good reason to do so and no other way to achieve the desired functionality
  – Delegate DNS domains to departments
  – Permit dynamic DNS updates except to special areas in the DNS tree
IP Anycast

- Anycast allows multiple servers to share a single IP
  - Network routing protocols select most appropriate server
- Requires special network configuration
- Requires special software on server
- Would probably not permit departments to do this
  - As requires access to core network routing protocols
- Protects against server or router failure
- Anycast DNS ‘server’ at 134.225.254.48
  - Physically two Infoblox appliances and one Linux VM
  - One at Earley Gate, one in ITS, one at Greenlands
Anycast DNS Examples
Anycast DNS Examples
Anycast DNS Examples
Anycast DNS Examples
Anycast DNS Examples
DHCP Myths

• IP addresses are not static / my address can change
  – Incorrect. By default we issue ‘sticky’ addresses, which is why we require the device’s MAC address

• I don’t know what my IP address is
  – Why does the average end user need to know?
  – Easy to find out even for those people with no knowledge
    • http://www.whatismyipaddress.com/

• IT Supporters cannot manage addresses
  – We are looking at this...
  – Where we can accommodate an IT supporter choosing a desired address (on their subnet!) for a machine, we will
DHCP Myths

- DHCP is unreliable
  - Once a device has an IP address lease, it is valid for a default of 7 days. The device will continue to work, even if DHCP becomes unavailable.
  - There are three ITS-managed DHCP servers on the network
    - Earley Gate, ITS, and Greenlands
  - The network actively protects against rogue DHCP servers
    - Switches block DHCP responses on edge ports
- “I don’t want ITS to know my MAC address”
  - We know it anyway!
  - Forwarding databases and ARP tables collected from routers and switches every 15 minutes and stored for auditing purposes
DHCP at UoR

- All hosts except IT Services managed servers should be registered with IT Services for DHCP
  - Chicken and egg situation
    - DHCP requires some servers to be available
    - But if servers configured to get IP address from DHCP and fail, they can’t get an IP address, so can’t be available, so can’t get an IP address...
  - IP address leases on campus are for 7 days by default
    - Except on guest networks where leases are for 4 hours
    - Lease time shortened if subnet will be changing
  - Change on previous policy which excluded departmental servers from DHCP registration
DHCP at UoR

- Advantages of DHCP to IT Supporters
  - No need to individually configure PCs
  - Users PCs can be registered on more than one subnet
  - No need to do anything when subnets get changed
  - No need to do anything when DNS / WINS servers get changed
  - ITS holds central inventory of MAC addresses
    - Which is also backed up off-site in two locations and on-site in four locations
  - We can offer more advanced services to assist you:
    - Staff image deployment via PXE boot (press F12 in BIOS)
    - Printer configuration files to secure your printers
    - Settings for Linux / Solaris install servers
  - Lets you spend more time helping users and less time on mundane tasks!
Questions?