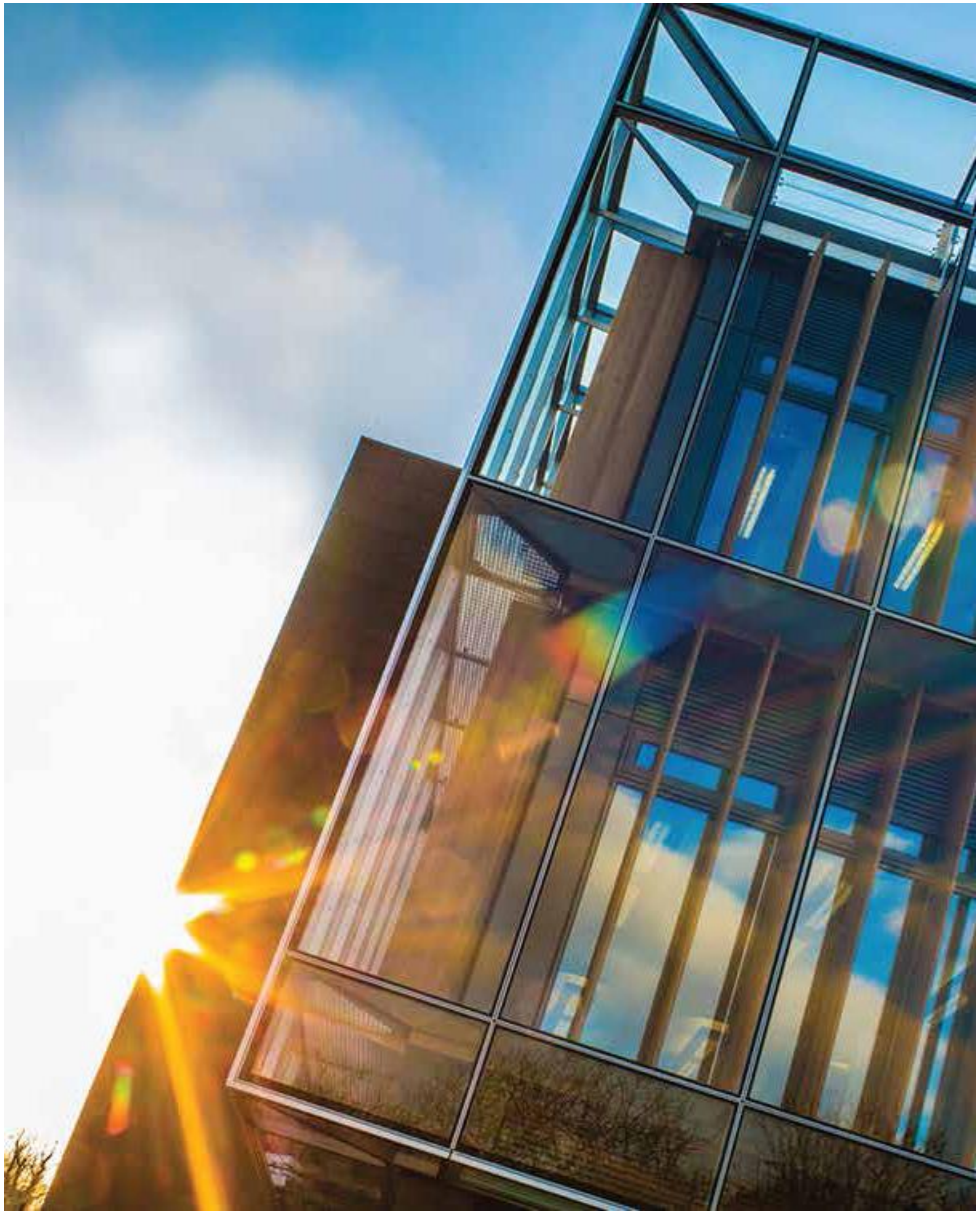
Maynooth University
National University of Ireland Maynooth

DHCP, DNS & IP Address Management

Bart Busschots



Outline

- The Back-story
  - How did we get to where we were?
  - What was the problem?
  - Why the need for change?
- Scope & Requirements
  - What must we have?
  - What would be nice to have?
- Our Solution
  - The over-all design
  - Each component in more detail
- How did it Go?
  - How did we migrate?
  - How have things changed?

Maynooth University
National University of Ireland Maynooth

The Back-story

A Long Time Ago …

- DHCP was initially deployed in the early 2000s
- Each device was assigned an IP (DHCP Reservation/Static Lease)
- A simple two-table database (‘*the host list*’) was maintained
  - A table of subnet data
  - A table of host data
- DHCP config, and Forward & Reverse DNS zones generated from *the host list*
- Single DHCP server
- Single pair of BIND DNS servers providing:
  - DNS Resolution for clients on campus
  - Hosting of public and private forward zones (using views)
  - Hosting of pubic and private reverse zones (using views)

The Cracks Begin to Show …

Implicit Assumptions

- Computers don’t move around
- One subnet per department, and computers don’t move between departments
- One-to-one-to-one mapping between IP addresses, MAC addresses, and hostnames
- Computers need static IPs & DNS names for peer-to-peer sharing (shared USB printers & local file shares)
- Only devices purchased by the University connect to the network

Modern Reality

- Staff carry devices with them from building to building all the time
- Many staff work for/with multiple departments
- Devices often connect via multiple MAC addresses (ethernet & WiFi)
- MAC addresses can move between devices (shared ethernet dongles)
- Peer-to-peer sharing is not a requirement anymore (replaced by central file shares, Office 365 etc.)
- Staff use many personally owned devices

Chickens Come Home to Roost …

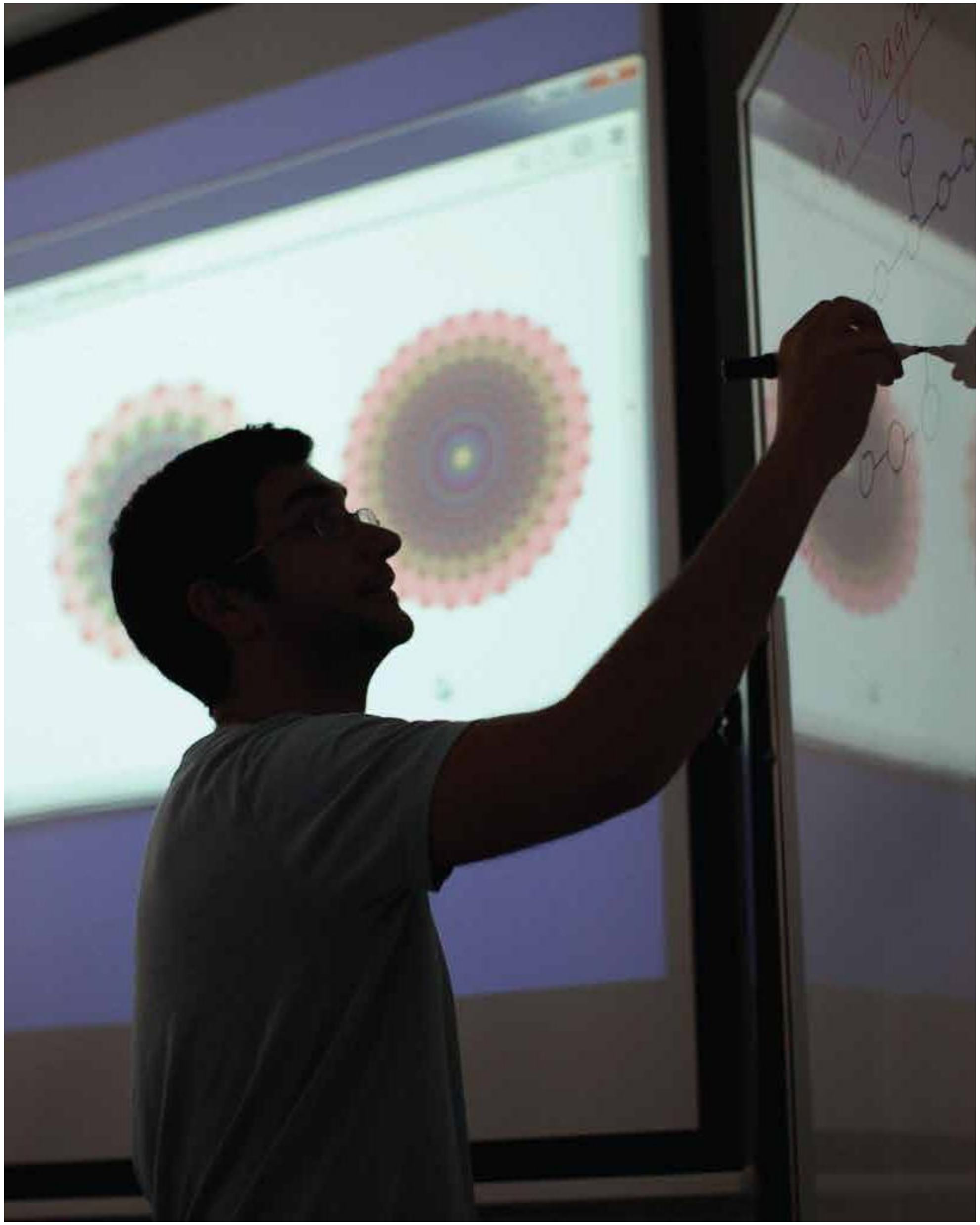
- Adding a new computers to the network was slow — calls had to be passed between sections within IT Services (User Support → Infrastructure → User Support)
- Reservations for all devices resulted in a false scarcity of IP addresses (total registered devices high, concurrent usage low)
- *Host list* could only store data for basic DNS records
  - All other DNS records were hand-coded into the zone files.
  - Usage of other kinds of DNS record increasing (particularly SRV & TXT)
- *Host list* couldn't deal with IPv6
- Becoming ever more brittle with age
  - Original developers no longer with the institution
  - Requirements drifted over time — scripts became ever more *hacky*
  - Only a small number of staff had the knowledge needed to hand-coded the DNS records not handled by *the host list*, or to deal with outages or problems

Creaks & Groans …

- DHCP Service provided by single physical server
  - No resilience
  - Outages each time the system needed to be patched
- DNS Resolution & Hosting of Authoritative Zones provided by single pair of master/slave BIND DNS Servers
  - Use of a single cluster for both hosting zones and DNS name resolution was once standard practice, but now considered insecure
  - Used BIND views which are not compatible with DNS SEC

Maynooth University
National University of Ireland Maynooth

Scope & Requirements



Needed

Delivered Services

- Resilient DNS name resolution
- Resilient hosting of authoritative DNS zones (public & private, and forward & reverse)
- Resilient DHCP service
- DDI management GUI for IT Services staff
- Granularly controlled access to DDI data for other stake holders, e.g. departmental technicians

Behind the Scenes

- Data stores to act as the single authoritative source for:
  - **IPv4** & **IPv6** info including **subnet definitions**, IP ranges for **DHCP pools**, **IP assignments** & per-subnet **DHCP options**
  - Authoritative **DNS records**
- The Data stores must have:
  - A well defined and documented format
  - One or more well documented APIs for querying and updating data
- Automatic generation (based on above data sources) of:
  - DHCP config
  - Reverse DNS zones

Wanted

- Low-cost— no realistic likely-hood of approval for significant budget (ruled out appliances)
- Open systems — no black boxes
  - Open source preferable
  - Well documented data storage schemes and APIs
- Widely used *‘Industry Standard’* systems
- Minimise custom scripting
  - Limit custom scripts to a middle-layer between ‘*standard’* systems
  - Focus on implementation of MU-specific business rules
  - Avoid direct manipulation of the raw data — use well documented APIs were ever possible

Maynooth University
National University of Ireland Maynooth

Our Solution

Components

Data Stores

- **php{IPAM}**
  - IPv4 & IPv6 IPAM
- **PowerDNS Server**
  - Forward DNS zones
  - *Blind Master* to Global & Local BIND clusters
- **MU DDI Config File (JSON)**
  - Config for all MU DDI Scripts

Middleware

- **MU DDI Scripts**
  - Auto-generate DHCP config
  - Auto-generate Reverse DNS Zones

Services Provided

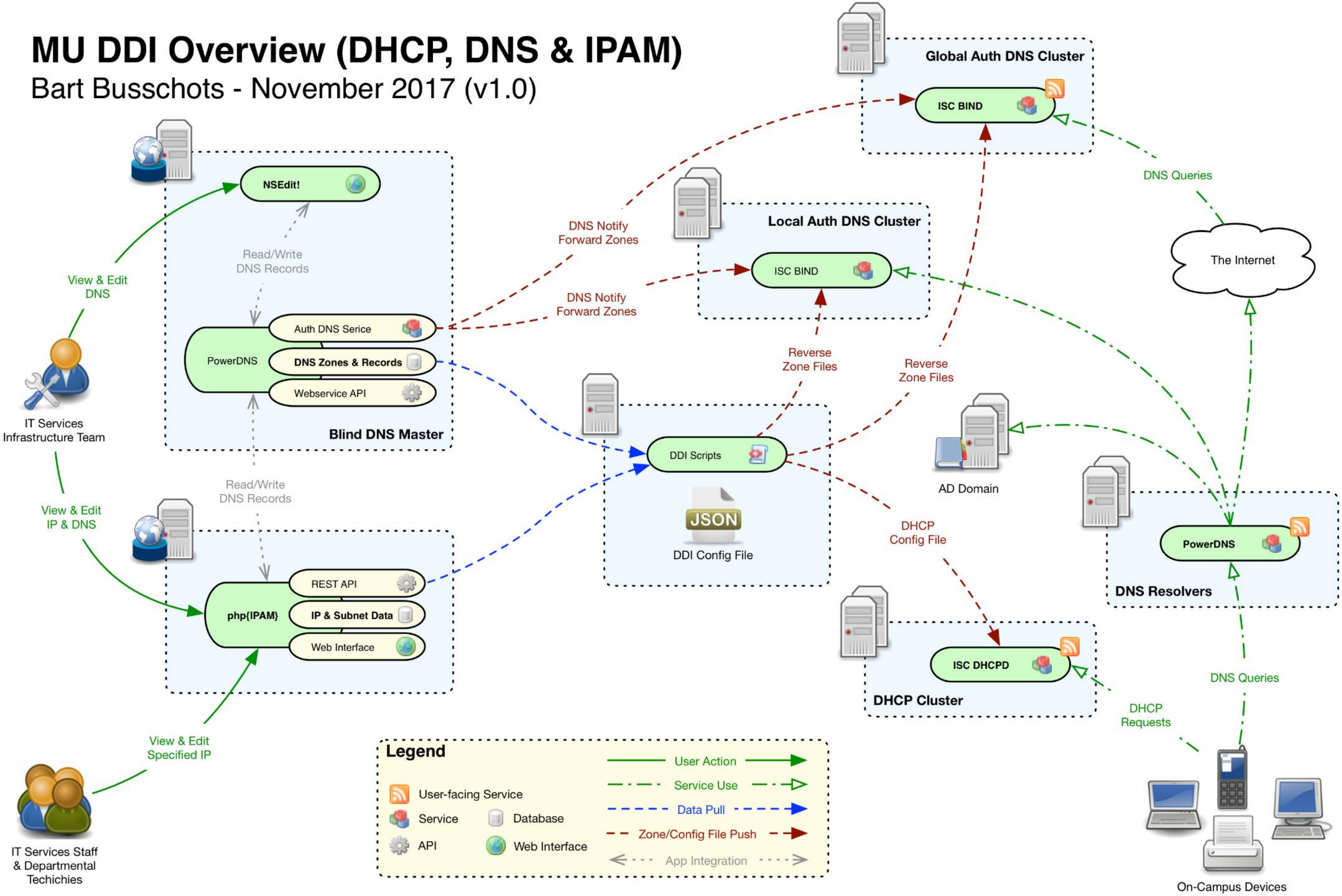
- DHCP — active-active **ISC DHCPD** cluster
- DNS Name Resolution — **PowerDNS Recursor**
- DNS Zone Hosting — 2 **ISC BIND** clusters
  - Global (public forward & reverse domains)
  - Local (private forward domains and private version of reverse domains)

Admin GUIs

- **php{IPAM}**
- **NSEdit**
- **MySQL Client of Choice**

MU DDI Overview (DHCP, DNS & IPAM)

Bart Busschots - November 2017 (v1.0)



Maynooth University
National University of Ireland Maynooth

IT Services

Domain Name Changes

Before

- Single forward domain with two views:
  - Public (served by default)
  - Private (served to MU IPs)
- Single public reverse zone with two views:
  - Public (served by default)
  - Private (served to MU IPs)
- Private reverse zones served to MU IPs only
- No Dynamic DNS

After

- Multiple public forward zones
- Dedicated *private* forward zone
  - Stub served from 3rd party cloud provider (needed for TLS certificates)
  - True zone served from *Local* BIND cluster
- Two distinct versions of public reverse zone
  - Public version served from *Global* BIND cluster
  - Private version served from *Local* BIND cluster
- Private reverse zones served from *Local* BIND cluster
- AD providing dynamic DNS on delegated private sub-domain

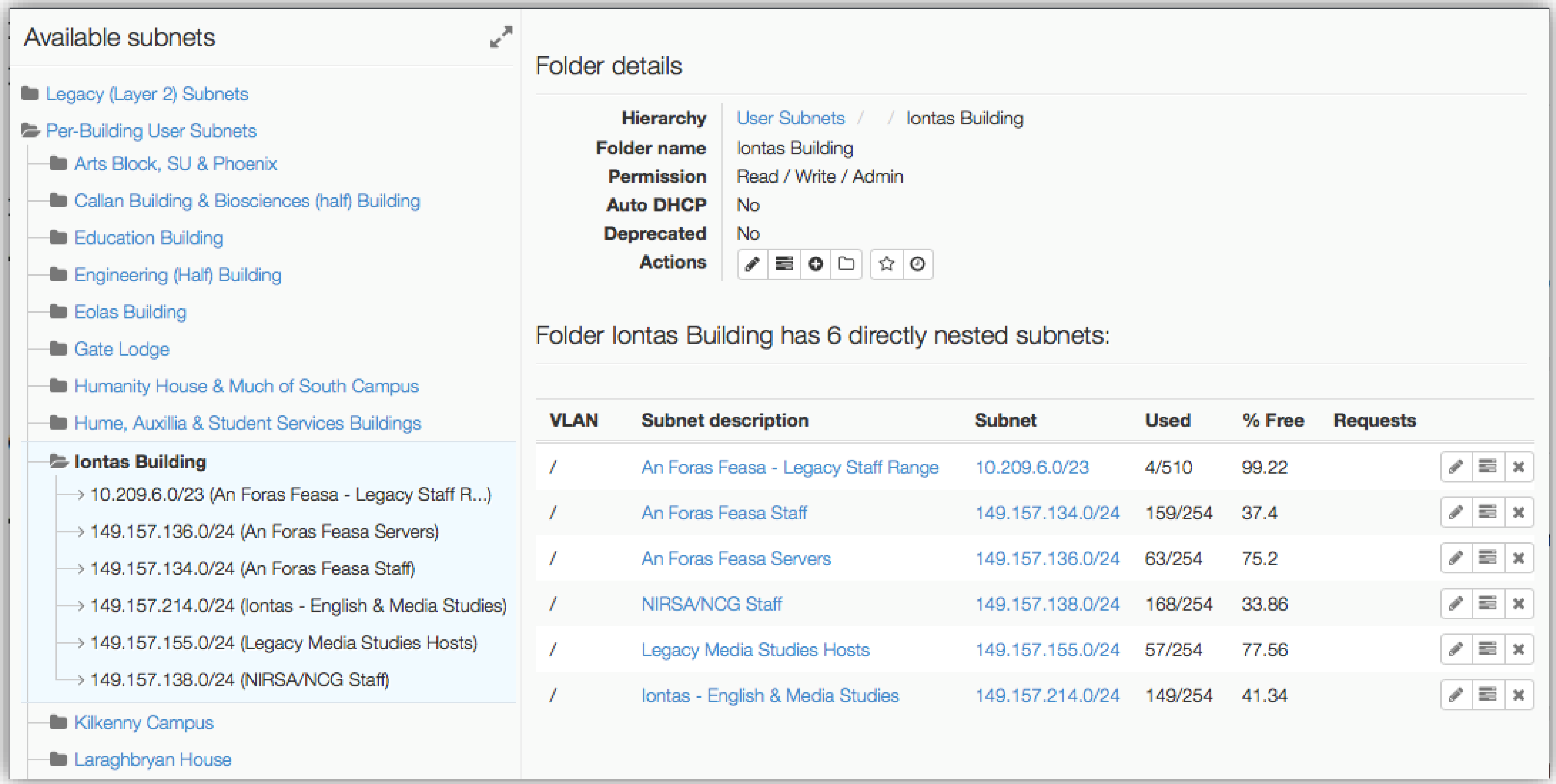
php{IPAM} — Features

- **Flexible hierarchical organisation of IPv4 & IPv6 data**
  - Sections contain subnets and/or folders
  - Folders can contain other folders or subnets
  - Subnets contain other subnets and/or folders and information on IPs
- Multiple **authentication** options including **AD**, **LDAP** & **Radius**
- **Roles** can be assigned at the section, folder, and subnet level
- **Custom fields** can be defined for most data objects, including **subnets**
- Each IP entry must be assigned a **tag**. The tag list is customisable.
- Built-in **change tracking** on IP entries (who, when, what to what)
- Basic **PowerDNS integration**
  - Surfaces DNS records for tagged IPs in the php{IPAM} GUI
  - Allows DNS records be created for tagged IPs
  - Provides UI for managing DNS zones &records, but chokes on large zones
- **Poor data validation**

php{IPAM} — Our Configuration

- Authentication via AD
- Subnets organised into Sections by team, e.g. *Voice, BMS, Data Centre, Wifi Clients* & *PACRs*
- Custom Fields on Subnets:
  - **Notes:** a free-form text area
  - **Auto DHCP:** a yes/no toggle to indicate whether or not to include the subnet in the auto-generated DHCP config
  - **DHCP Options:** a free-form text area for specifying subnet-specific DHCP options, e.g. phone config options
  - **Deprecated:** a flag to indicate that the subnet is in the process of being decommissioned (no new devices should be added to it)
- Tags in use:
  - Standard tags: *Used* & *Reserved*
  - Custom tags: *DHCP Pool, DHCP Reservation* & *Managed by 3rd Party*

php{IPAM} UI — Section View



Available subnets

- Legacy (Layer 2) Subnets
- Per-Building User Subnets
  - Arts Block, SU & Phoenix
  - Callan Building & Biosciences (half) Building
  - Education Building
  - Engineering (Half) Building
  - Eolas Building
  - Gate Lodge
  - Humanity House & Much of South Campus
  - Hume, Auxilia & Student Services Buildings
  - **Iontas Building**
    - 10.209.6.0/23 (An Foras Feasa - Legacy Staff R...)
    - 149.157.136.0/24 (An Foras Feasa Servers)
    - 149.157.134.0/24 (An Foras Feasa Staff)
    - 149.157.214.0/24 (Iontas - English & Media Studies)
    - 149.157.155.0/24 (Legacy Media Studies Hosts)
    - 149.157.138.0/24 (NIRSA/NCG Staff)
  - Kilkenny Campus
  - Laraghbryan House

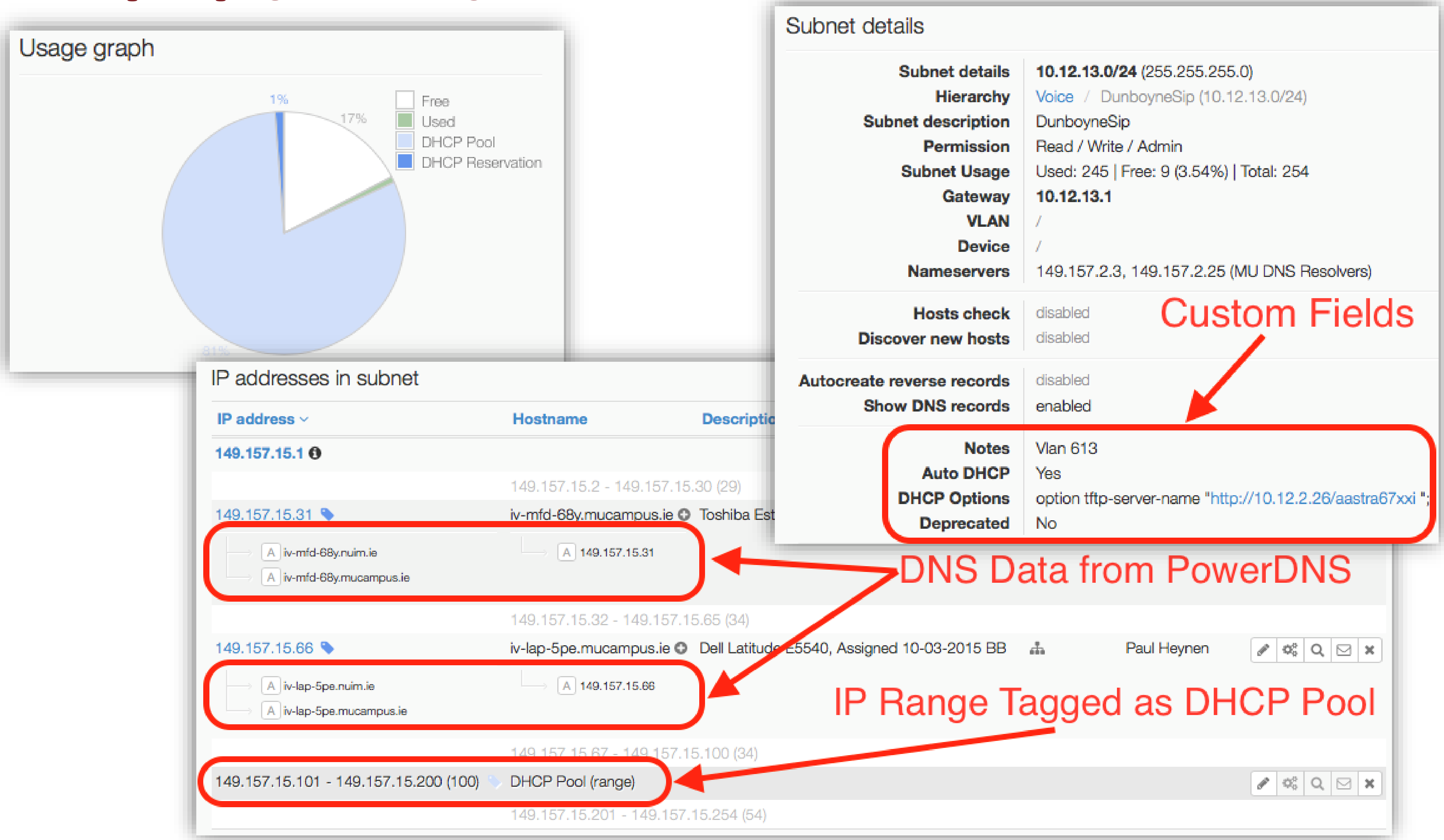
Folder details

Hierarchy	User Subnets / / Iontas Building
Folder name	Iontas Building
Permission	Read / Write / Admin
Auto DHCP	No
Deprecated	No
Actions	

Folder Iontas Building has 6 directly nested subnets:

VLAN	Subnet description	Subnet	Used	% Free	Requests
/	An Foras Feasa - Legacy Staff Range	10.209.6.0/23	4/510	99.22	
/	An Foras Feasa Staff	149.157.134.0/24	159/254	37.4	
/	An Foras Feasa Servers	149.157.136.0/24	63/254	75.2	
/	NIRSA/NCG Staff	149.157.138.0/24	168/254	33.86	
/	Legacy Media Studies Hosts	149.157.155.0/24	57/254	77.56	
/	Iontas - English & Media Studies	149.157.214.0/24	149/254	41.34	

php{IPAM} UI — Subnet View



Subnet details

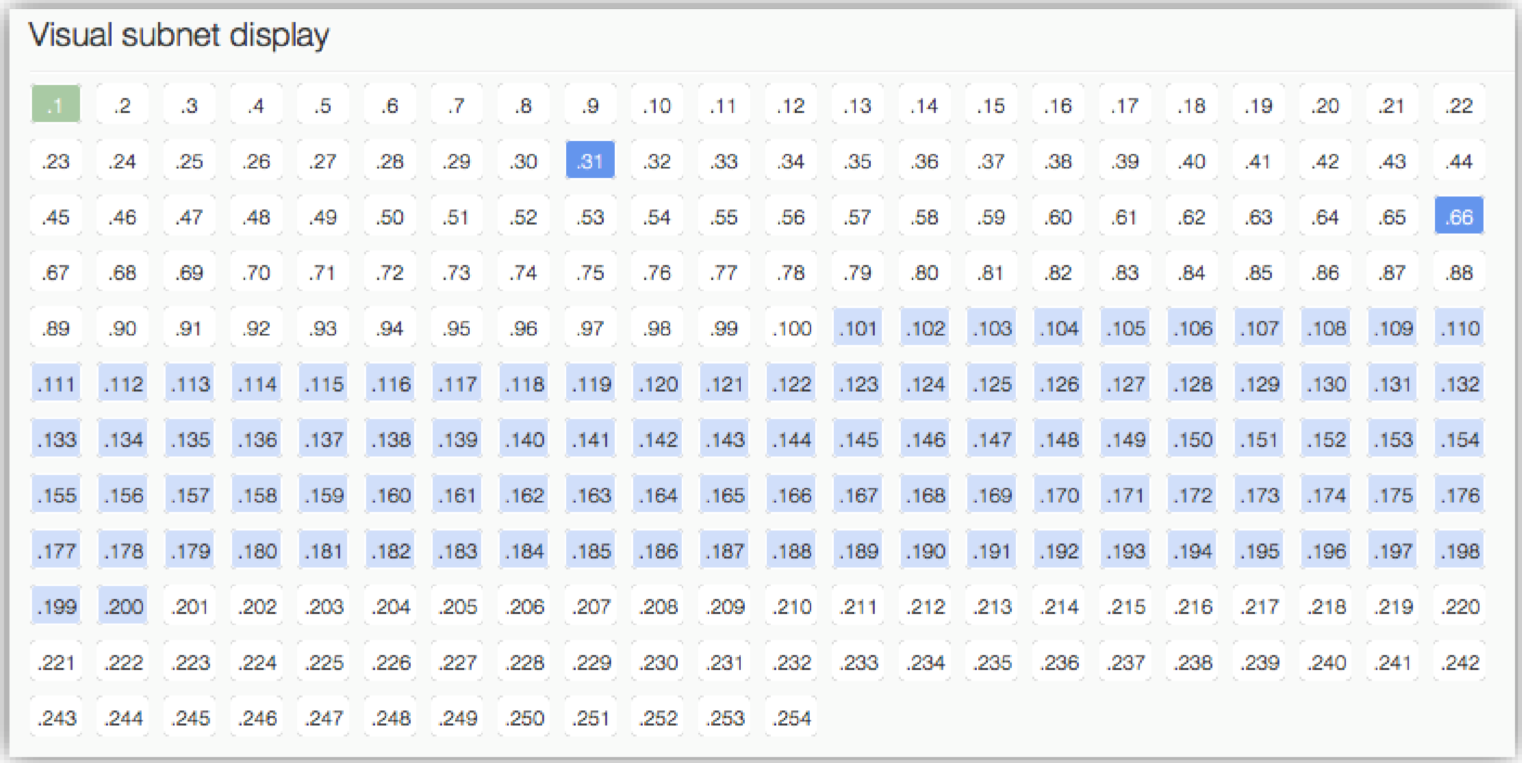
Subnet details	**10.12.13.0/24** (255.255.255.0)
Hierarchy	Voice / DunboyneSip (10.12.13.0/24)
Subnet description	DunboyneSip
Permission	Read / Write / Admin
Subnet Usage	Used: 245 | Free: 9 (3.54%) | Total: 254
Gateway	**10.12.13.1**
VLAN	/
Device	/
Nameservers	149.157.2.3, 149.157.2.25 (MU DNS Resolvers)
Hosts check	disabled
Discover new hosts	disabled
Autocreate reverse records	disabled
Show DNS records	enabled
Notes	Vlan 613
Auto DHCP	Yes
DHCP Options	option tftp-server-name "http://10.12.2.26/aastra67xxi ";
Deprecated	No

IP addresses in subnet

IP address	Hostname	Descriptio			
149.157.15.1					
	149.157.15.2 - 149.157.15.30 (29)				
149.157.15.31	iv-mfd-68y.mucampus.ie	Toshiba Est			
A iv-mfd-68y.nuim.ie A iv-mfd-68y.mucampus.ie	A 149.157.15.31				
	149.157.15.32 - 149.157.15.65 (34)				
149.157.15.66	iv-lap-5pe.mucampus.ie	Dell Latitude E5540, Assigned 10-03-2015 BB		Paul Heynen	
A iv-lap-5pe.nuim.ie A iv-lap-5pe.mucampus.ie	A 149.157.15.66				
	149.157.15.67 - 149.157.15.100 (34)				
149.157.15.101 - 149.157.15.200 (100)	DHCP Pool (range)				
	149.157.15.201 - 149.157.15.254 (54)				

Maynooth University
National University of Ireland Maynooth

php{IPAM} UI — Subnet View



Visual subnet display

.1	.2	.3	.4	.5	.6	.7	.8	.9	.10	.11	.12	.13	.14	.15	.16	.17	.18	.19	.20	.21	.22
.23	.24	.25	.26	.27	.28	.29	.30	.31	.32	.33	.34	.35	.36	.37	.38	.39	.40	.41	.42	.43	.44
.45	.46	.47	.48	.49	.50	.51	.52	.53	.54	.55	.56	.57	.58	.59	.60	.61	.62	.63	.64	.65	.66
.67	.68	.69	.70	.71	.72	.73	.74	.75	.76	.77	.78	.79	.80	.81	.82	.83	.84	.85	.86	.87	.88
.89	.90	.91	.92	.93	.94	.95	.96	.97	.98	.99	.100	.101	.102	.103	.104	.105	.106	.107	.108	.109	.110
.111	.112	.113	.114	.115	.116	.117	.118	.119	.120	.121	.122	.123	.124	.125	.126	.127	.128	.129	.130	.131	.132
.133	.134	.135	.136	.137	.138	.139	.140	.141	.142	.143	.144	.145	.146	.147	.148	.149	.150	.151	.152	.153	.154
.155	.156	.157	.158	.159	.160	.161	.162	.163	.164	.165	.166	.167	.168	.169	.170	.171	.172	.173	.174	.175	.176
.177	.178	.179	.180	.181	.182	.183	.184	.185	.186	.187	.188	.189	.190	.191	.192	.193	.194	.195	.196	.197	.198
.199	.200	.201	.202	.203	.204	.205	.206	.207	.208	.209	.210	.211	.212	.213	.214	.215	.216	.217	.218	.219	.220
.221	.222	.223	.224	.225	.226	.227	.228	.229	.230	.231	.232	.233	.234	.235	.236	.237	.238	.239	.240	.241	.242
.243	.244	.245	.246	.247	.248	.249	.250	.251	.252	.253	.254										

PowerDNS Suite (2 Distinct Products)

PowerDNS Recursor

- Features
  - Provides **DNS name resolution**
  - Light-weight & fast
  - Easy to configure
- Our Configuration
  - Cluster of two resolvers
  - Configured Forwarding Zones:
    - AD domain forwarded to DCs
    - Private MU domains forwarded to *Local* BIND cluster
    - MU reverse zones forwarded to *Local* BIND cluster

PowerDNS Server

- Features
  - Provides **hosting of DNS zones**
  - Supports multiple storage back-ends including RDBMSes
  - Compatible with BIND
  - Lightweight & fast
  - Easy to configure
- Our configuration
  - Single server
  - MySQL backend
  - *Blind master* to both *Global* and *Local* BIND clusters for all forward zones

PowerDNS Server GUIs

NSEdit!

- Free open-source PHP webapp
- View, edit & add zones and records
- UI works well for managing zones and adding records
- Good data validation when adding records
- UI works poorly for managing records with large domains — no search feature, just alphabetic list of records

MySQL Clients

- Table structure is very intuitive
- Generic MySQL client with search and filter features is often the quickest way to interact with PowerDNS

Other Open Source Components

ISC BIND

- *De-facto* Industry standard DNS server
- Robust & Full-featured
- Many years of experience with BIND in MU

ISC DHCPD

- *De-facto* Industry standard DHCP Server
- Robust & Full-featured
- Support for active-active clustering
- Many years of experience with DHCPD in MU

Our Scripts — “MU DDI Scripts”

- Middleware between the open-source components to implement MU business rules
  - Automatically generate & deploy DHCPD config
  - Automatically generate & deploy *global* and *local* versions of reverse DNS zones
  - Utility scripts
- Written in Perl
- Interaction with the open-source components through REST APIs and other officially supported and well documented mechanisms
- Actions and errors logged to central syslog server
- No *magic numbers* — all variables defined in single JSON-formatted config file (*the DDI Config file*)

DHCP Config Auto-Generation

- Generated config based on data in php{IPAM} & DDI config file
- Algorithm:
  1. Generate config file
  2. Validate generated config with `dhcpd -t -cf`
  3. Verify that both DHCP nodes are up with `dhcping`
  4. SFTP generated config to both nodes
  5. Re-start DHCPD on secondary, then primary via `systemd`
  6. Verify both nodes came back up with `dhcping`

DHCP Config Auto-Generation

- Generated config consists of three logical sections:
  1. Global settings (from DDI config file)
  2. Subnet declarations (from php{IPAM}, including our custom fields)
  3. Host declarations (from php{IPAM})
- Generated config heavily commented to make it human-readable for debugging purposes
  - Comments specify the source of the various pieces of information

DHCPD Config Snippet

```
#
# -- Subnet 149.157.7.192/26 (php{IPAM} id=224) --
#
# Description: Computer Science Servers
subnet 149.157.7.192 netmask 255.255.255.192{
  # -- Local Parameters --
  authoritative; # hard-coded
  option broadcast-address 149.157.7.255; # derived
  option routers 149.157.7.193; # from php{IPAM}

  # -- Custom Name Servers (from php{IPAM}) --
  option domain-name-servers 149.157.246.30;

  # -- Custom DHCP Options (from php{IPAM}) --
  option domain-search "cs.nuim.ie";
  option domain-name "cs.nuim.ie";

  # -- Dynamic IP Pool (from php{IPAM}) --
  pool{
    failover peer "mu_dhcp"; # from DDI config file
    range 149.157.7.247 149.157.7.254;
  }
}
```

Reverse DNS Zone Generation

- Multiple zone files need to be generated
- Generated zone files based on PowerDNS and DDI config file
- Algorithm (repeated for each needed zone file)
  1. Generate zone file
     - DDI config file defines which domains should be treated as *private*
     - DDI config file defines zone weightings for automatic conflict resolution between multiple `A` records for the same IP
  2. Validate generated file with `named-checkzone`
  3. SFTP generated file to *Local* or *Global* BIND master
  4. Trigger a zone reload via `rndc`

Utility Scripts

- Perform data integrity checks
  - Flag **single-field data validation issues** not dealt with by php{IPAM} (e.g. invalid MAC addresses or hostnames)
  - Flag **data integrity problems between records** (e.g. inconsistent mappings between MAC addresses and hostnames)
  - Flag **orphaned and obsolete records** (e.g. A records pointing to IPs within DHCP pools)
  - Flag inconsistencies between authoritative NS records for sub-domains and NS records returned by the delegated-to servers
- Bump the serial on all published domains
- Flush the caches on all resolvers

Maynooth University
National University of Ireland Maynooth

How did it Go?

The Big Change …

- Old and new infrastructure run in parallel (each DNS zone and subnet only served from one system at a time)
- Migration Process
  - DNS Resolvers deployed first
    - Legacy and new DHCP servers updated to point all clients at the new resolvers
    - DNS recursion disabled on legacy DNS (addressing auth+recurse security issue)
  - DHCP & Authoritative DNS Migrated in parallel
    - DHCP moved one subnet at a time by copying the data then changing the helper address on the router
    - Authoritative DNS moved one domain at a time (PowerDNS import from BIND zone file) then NS records and/or Forwarding zones updated

What’s Improved?

- From our Staff’s point of view:
  - Basic network connectivity ‘just works’ — no DHCP or DNS outages
  - Can move freely between buildings & departments with their devices
  - Can more easily use personally owned devices
  - Orders for University-owned devices processed more quickly
- From IT Services’ point of view:
  - ‘Single pane of glass’ for all IPv4 & IPv6 network information
  - Reduction in work-load — very few devices need reservations, and more staff can now deal with the remaining few requests
  - Maintenance is easier because any single VM can be rebooted without triggering outages on any user-facing services
- From Departmental Technicians’ Point of view:
  - Visibility into the configuration of and IP usage of the subnets relevant to them

Maynooth University
National University of Ireland Maynooth

Questions?