

Service Discovery

ITL

DNS-Based Service Discovery

- DNS SRV records [RFC 2782]
 - e.g. an SRV record for "_http._tcp.example.com." lists all address/port combinations for http servers reachable by TCP in the example.com. domain
- That assumes that the user wants **any** web server in "example.com"; not a likely scenario.
- DNS-SD adds one level of indirection to allow a named list of services that can be presented to the user

DNS-SD

-
- Query for PTR records (instead of SRV)
 - query for PTR with name `_ipp._tcp.example.com`.
 - get a list of `<instance>.<service>.<domain>`
 - e.g.
 - “Color Printer - Sales. `_ipp._tcp.example.com`.”
 - “Slow Printer (Sally). `_ipp._tcp.example.com`.”
 - Give the user a list of options, user selects
 - Issue SRV query to get the actual IP and port number for the selected instance
 - Issue TXT query for additional parameters (e.g. printer queue name)

Production Examples

- Apple - Bonjour
 - Target: Small networks and work groups
 - Combined with mDNS
 - Recently expanded to use dynamic DNS servers
- Microsoft - Active Directory
 - Target: Enterprise Networks
 - Combined with Dynamic DNS (DDNS)
 - Part of an Enterprise-wide authentication and resource management system

Microsoft

- Active Directory
- Windows 2000, XP, 2003, Vista, Server 2008
 - Core protocols:
 - Dynamic DNS
 - LDAP
 - Service Discovery
 - Kerberos
- Hierarchical name space (based on DNS)
- Multi-master peer database replication

Dynamic DNS

- Client or DHCP server modify DNS when the client gets an IP address
 - In AD the client sends the update request
 - Standard requires DNSSEC
 - AD uses internal ACLs instead
- Servers update DDNS based on the roles they acquire and the services they can provide
- *Side Note: this is a different mechanism than the web based service(s) by similar names, e.g. DynDNS.*

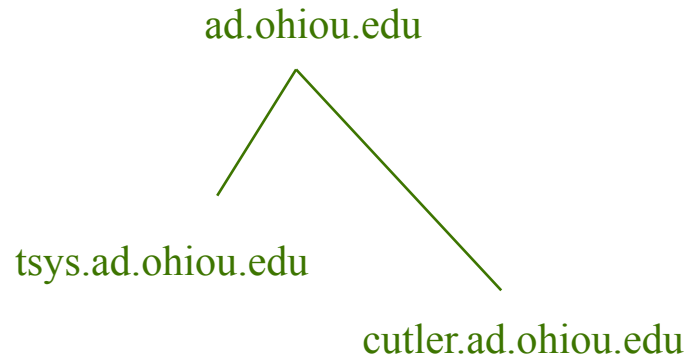
LDAP

- Light-weight Directory Access Protocol
 - Based on the structure of ISO X.500
 - Compatible with X.500 data schemas
 - Does not rely on ISO protocols
- Example of an RDN (relative distinguished, aka unique within a container, name in LDAP)
 - CN=Steve Kille, O=Isode Limited, C=GB

Active Directory Structure

- Domain Tree

- Hierarchy
- Higher levels control lower levels



- Forest

- Collection of domain trees
- Implied trust relationship

- Explicit trust relationships

- Between forests

Service Discovery in AD

- Based on DNS SRV records
- For Example, the general catalog server:
 - `_gc._tcp.mycorp.com. 600 IN SRV 0 100 3268 moose.mycorp.com.`
- LDAP Servers:
 - `_ldap._tcp.mycorp.com. 600 IN SRV 0 100 389 moose.mycorp.com.`
- There can be many SRV records for a service
- AD uses SRV records for
 - General Catalog servers
 - Kerberos
 - Domain Controllers

DNS SRV Records

RFC 2782

```
- _ldap._tcp.mycorp.com. 600 IN SRV 0 100 389 moose.mycorp.com.
```



- Service.Proto.Name TTL Class SRV Priority Weight Port Target
 - Priority
 - Hosts with the lowest priority must be used first
 - Weight
 - If hosts are listed with the same priority, select randomly among those hosts, using weight to bias the selection (load balancing)