



# **COSC301**

## Lecture 12: Dynamic Host Configuration & Service Discovery

# IP Addr. Assignment

- 📌 First there was Reverse ARP (RARP)
  - 📌 Only IP address, no options for DNS etc.
- 📌 Then the Bootstrap Protocol (BOOTP)
  - 📌 Included concept of tagged options
  - 📌 Useful for software like X-Terminals,
  - 📌 Allow direct network booting
  - 📌 Like RARP, constrained to single subnet, but perform at UDP/IP, instead of MAC layer

# DHCP

- Dynamic Host Configuration Protocol (DHCP)
- Compatible with BOOTP (uses same ports)
- Can efficiently use a shared pool of addresses
- IP addresses can be tied to MAC address, or Client ID
- Ubiquitous (at least in the IPv4 sense!)
- Limited to a single subnet, but routers can incorporate relay agents
- Successor: DHCPv6, less useful in IPv6

# How DHCP Works

- 📌 Client broadcasts UDP request to 255.255.255.255 port 67
  - 📌 Routers can relay using a relay agent
- 📌 The first DHCP server may send an offering
  - 📌 Corollary: there should usually only be one DHCP server in a subnet (broadcast zone)
- 📌 Offer can contain many types of options, like router/gateway and DNS server
  - 📌 See <https://tools.ietf.org/html/rfc2132> for detail

# Security of DHCP

- 📌 rogue DHCP server
  - 📌 You will get wrong gateway and DNS server under the attacker's control
- 📌 No authentication for clients
  - 📌 Anyone can get IP addr. and join the network
  - 📌 IP addr. depletion attack

# Manual vs. DHCP

- 📌 You could do it manually. Why not?
  - 📌 **PRO** Protection against multiple/rogue DHCP servers!
  - 📌 **CON** Change management
  - 📌 **PRO / CON:** Better control, but bigger problems when mistakes are made
- 📌 DHCP is still fairly reliable. *Short* outages are generally unnoticeable

# Static vs. Dynamic

- 📌 Static address is assigned by system admin in the DHCP configuration file using the client's MAC address
  - 📌 Server machines' addresses should be manual or static
- 📌 Dynamically allocated addresses have a lease time period before they are re-assigned
- 📌 Automatically allocated address can be assigned to the same client as it keeps a table of past IP addresses and their clients MAC addresses.
- 📌 Dynamic change of IP addr. breaks existing connections
  - 📌 Beware downloaders, terminal sessions



# Ad-hoc IP Addressing

- 🔊 ZeroConf (Zero Configuration Networking)  
Link Local Addresses
  - 🔊 169.254.0.0/16
  - 🔊 Single subnet, no routing (no internet)
- 🔊 Get an address by selecting an address and testing for duplicates
- 🔊 Useful for ad-hoc networks, and unconfigured network devices
- 🔊 Best supported on Mac OS X (anecdotally)



# Ad-hoc Name Resolution

- 📍 IP traditionally lacks this
  - 📍 Proprietary LAN-based protocols have supported it for years
    - 📍 AppleTalk, NetBIOS
- 📍 Useful when infrastructure has no local knowledge (e.g. no DNS)
- 📍 In IP world: Multicast DNS (mDNS) as part of ZeroConf

# Multicast DNS

- mDNS queries are the same as DNS, except queries are targeted at 224.0.0.251:5353
  - Queries are made under '.local', so '.local' should never be used for traditional DNS
    - <device\_name>.local.
  - Client resolvers must recognise .local queries
    - Special treatment: not upstream DNS
- Also Microsoft's LLMNR (Link-Local Multicast Name Resolution)

# Service Discovery

- 📌 Locate the services, e.g. email or web server in a domain, we need automatically, or by browsing, searching/filtering or provisioning
  - 📌 Indistinct services all behave the same way and can be assigned automatically
  - 📌 Distinct services provide different behavior and need to be browsed, searched, or provisioned
- 📌 Need to consider network context
  - 📌 Operates within a specified network scope
- 📌 Many protocols were proposed for service discovery
  - 📌 DNS-SD in Zero Configuration Networking, DHCP options, SLP, Directory Services like LDAP

# Motivations

- 📌 Why auto service discovery?
  - 📌 Centralised Administration
    - 📌 Faster to fix, but a point of failure
  - 📌 Lower support costs
    - 📌 Less on-site reconfiguration
  - 📌 Enhanced network mobility, plug & play

# Software Support

- Either program uses API to discover services
  - Live configuration, change detection, better user experience
- ... or external program modifies software configuration, then reloads server
  - Useful for services that do not require reconfiguration during runtime. e.g. configuration via DHCP options.
  - Also useful for retro-fitting

# Well-known D.N.s

- 📌 `http://wpad.domain/wpad.dat` for Web proxy auto-configuration
- 📌 Other common names include `smtp` (or `mail`), `pop3`, `imap`, `ftp`, `www`, `ns1`, `ns2`, `time`
  - 📌 These should be aliases, so they can be redirected to other machines easily
- 📌 Most useful for human-based configuration

# S.D. with DHCP

- 🔊 DHCP has various, diverse options: Syslog, DNS, LPR, WINS, NTP, LDAP (!)
  - 🔊 Think carefully about security
- 🔊 Requires client support, in DHCP client or application
- 🔊 You can provision based on the machine or subnet, or a single group



# S.D. with DNS-SD

- Service (SRV) records specify service type, transport protocol, and the domain.
- `_smtp._tcp.domain` returns Priority, Weight, Port and Address of mail servers, for browsing.
  - DNS Service Discovery (DNS-SD) allows for browsing service instances.
  - Most commonly used with mDNS.
- Not suitable for very dynamic data in traditional DNS. Why?

# DNS-SD Example

- 📌 Examples taken from draft DNS-SD standard.
- 📌 What services are available on dns-sd.org?  
(provides a discovery starting point)  
`dig +short -t any _services._dns-sd._udp.dns-sd.org`  
`_ftp._tcp.dns-sd.org.`  
`_ssh._tcp.dns-sd.org. (and others...)`
- 📌 What FTP services are available on dns-sd.org?  
`dig +short -t any _ftp._tcp.dns-sd.org`  
`Apple\032QuickTime\032Files._ftp._tcp.dns-sd.org.`  
(and others...)

# DNS-SD Example

 How do I access “Apple QuickTime Files”?  
host -t any "Apple QuickTime  
Files.\_ftp.\_tcp.dns-sd.org"  
Apple\032QuickTime\032Files.\_ftp.\_tcp.dns-sd.org  
SRV 0 0 21 ftp.apple.com.  
Apple\032QuickTime\032Files.\_ftp.\_tcp.dns-sd.org  
text "path=/quicktime"

 ... i.e. FTP to [ftp.apple.com/quicktime](ftp://ftp.apple.com/quicktime)

# SLP for S.D.

- Service Location Protocol enumerates by searching for service type and attributes
- Devices operate within a scope, and have service-agents, which advertise the service to user-agents, which themselves act as a client service on the local machine
  - Directory-agents gather all the information in a scope for fast retrieval on large networks
- Used mostly in Novell's IP offerings, and enterprise-grade (LAN) printers



# Security

- Can give information about network infrastructure to attackers who might otherwise be going in “blind”... do we care?
  - But never rely on blindness (security through obscurity)
- Additional attack vectors
  - Race-conditions with DHCP
  - Can we authenticate DHCP servers?
  - DNS, Gateway, ... LDAP

# S.D. w/ Directory Services

- 📍 Directory services commonplace in managed networks: Microsoft Active Directory, Novell eDirectory, Apple Open Directory, LDAP
- 📍 A directory is represented as a tree; contains objects such as users, servers, print queues, applications and client machines
- 📍 Users authenticate to the tree/domain, and can view the objects in them
  - 📍 Access control is a central subject

# Summary

-  Pros and cons of DHCP compared with manual assignment.
-  Security issues of DHCP



# Reading



*Cisco SAFE Layer 2 Security In-depth  
Version 2*

[http://www.cisco.com/warp/public/cc/  
so/cuso/epso/sqfr/sfblu\\_wp.htm](http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/sfblu_wp.htm)