honest Consulting

DHCP Security Workshop

prepared for DDI User Group

by Andreas Taudte // honest consulting GmbH

on December 2, 2021

Presentation Outline

1. DHCP in a Nutshell
2. DHCPv6 in a Nutshell
3. DHCP Redundancy
4. Influencers of DHCP
5. Hardening of DHCP
6. DHCP Troubleshooting

DHCP in a Nutshell

Dynamic Host Configuration Protocol

- Bootstrap Protocol (BOOTP) defined in RFC 951
- DHCP defined in RFC 2131
- Server Port 67/UDP
- Client Port 68/UDP
- Manual: specific IP address assigned to certain Client
- Dynamic: dynamical Assignment from Range of Addresses
- Automatic: permanent Assignment from Range of Addresses

DHCP Message Format

- **op** Request (1) or Reply (2)
- **hops** Number of Relays on the Path
- **ciaddr** Client's IP Address
- **yiaddr** given IP Address (if ciaddr 0.0.0.0)
- **siaddr** Server's IP Address
- **giaddr** Relay's IP Address
- **chaddr** Client's MAC Address

op	htype	hlen	hops
xid			
sec		flags	
ciaddr			
yiaddr			
siaddr			
giaddr			
chaddr			
sname			
file			
options			

Table 1: DHCP Message Format

The DORA Process

- **D**iscover **O**ffer **R**equest **A**cknowledgement

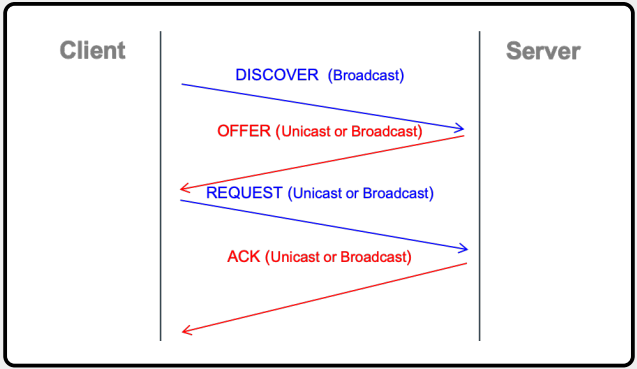

Figure 1: The DORA Process

DHCP Relay Agents (aka IP Helper)

- Relay Agents pass Messages between Clients and Servers

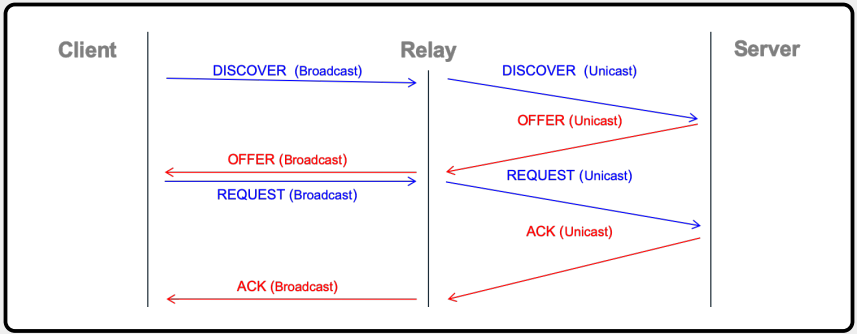

Figure 2: DHCP Relay Agents (aka IP Helper)

DHCP Lease Times

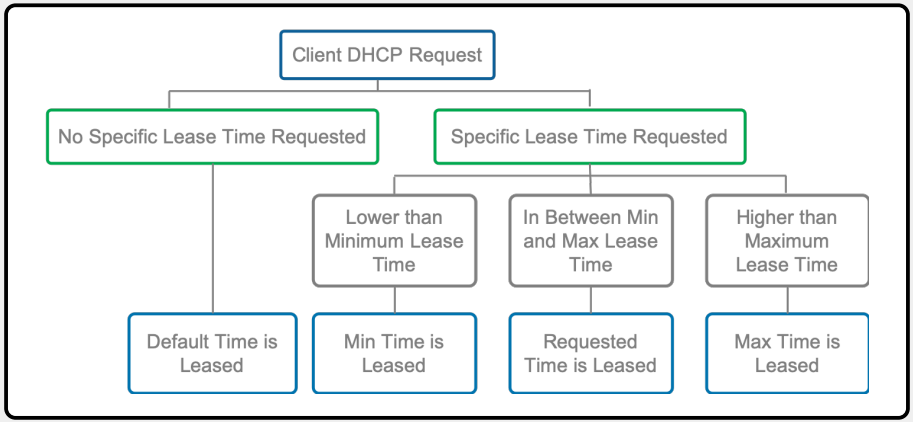

Figure 3: DHCP Lease Times

T1 and T2

- Controls how Leases are extended and when expiring
- **T1**: Time after Client tries to extent Lease with DHCP Server
  - RENEWING via Unicast
- **T2**: Time after Client tries to extent Lease with any DHCP Server
  - REBINDING via Broadcast
- Client sends DHCPREQUEST in both Cases
- T1 < T2 < Lease Expiry Time
  - T1 = 0,5 * Lease Time
  - T2 = 0,875 * Lease Time

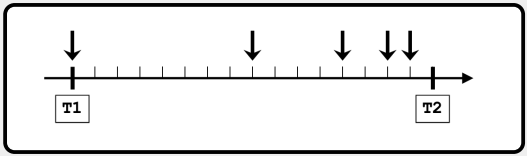

Figure 4: T1 and T2

Client States

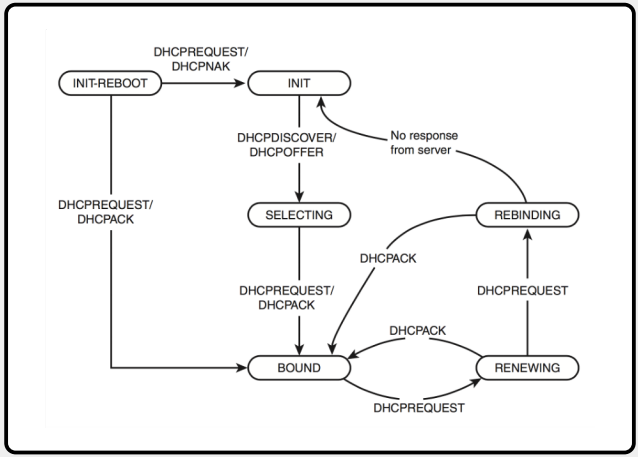

Figure 5: Client States

DHCPv6 in a Nutshell

Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

- **Motivation**
  - DHCP allows centralized Control and Auditing of assigned IP Addresses
- Updated Version of IPv4's DHCP
  - Supports IPv6 Addressing and Configuration Specification
  - Process is comparable to IPv4
- Client detects Presence of Router(s) on its Link
  - Router found: Router Advertisement (RA) to determine if DHCP can be used
  - No Router found: Solicit Message to All-DHCP-Agents (Multicast) Address
- Clients listen on 546/UDP
- Servers and Relay Agents listen on 547/UDP

DHCPv6 Principles

- Stateless Address Auto-Configuration (RFC 4862)
  - Server doesn't assign Address but provides Configuration Parameters
  - Similar to DHCPv4 DHCPINFORM/DHCPACK
- Stateful Configuration (RFC 8415)
  - Server assigns Address and provides Configuration Parameters
- Prefix Delegation (RFC 3769)
  - Server delegates Prefixes Routers instead of leasing Addresses
- Special Multicast Addresses
  - FF02::1:2 = All-DHCP-Agents[1]
  - FF05::1:3 = All-DHCP-Servers[2]

[1] used by Client to communicate with on-link Relay Agents and Servers

[2] used by Relay Agent to communicate with Servers

DHCP Unique Identifier (DUID)

- Used by Client and Server to identify each other
- Should not change over Time
- 3 Types of DUID
  - Link-Layer Address plus Time (DUID-LLT)
  - Vendor-assigned unique ID based on Enterprise ID (DUID-EN)
  - Link-Layer Address (DUID-LL)
- Identity Association (IA)
  - Construct to identify, group and manage Set of related IP Addresses
  - Client associates IA for each Interface with DHCP-assigned Address (IAID)
  - Associated with exactly one Interface
  - Consistent across Restarts by the Client

DHCPv6 Messages vs. DHCPv4 Messages

DHCPv6 Message (Type)	**DHCPv4 Message**
Solicit (1)	DHCPDISCOVER
Advertise (2)	DHCPOFFER
Request (3), Renew (5), Rebind (6)	DHCPREQUEST
Reply (7)	DHCPACK / DHCPNAK
Release (8)	DHCPRELEASE
Information-Request (11)	DHCPINFORM
Decline (9)	DHCPDECLINE
Confirm (4)	-
Reconfigure (10)	DHCPFORCERENEW
Relay-Forw (12), Relay-Reply (13)	-

Table 2: DHCPv6 Messages vs. DHCPv4 Messages

DORA becomes SARR

- **S**olicit **A**dvertise **R**equest **R**eply

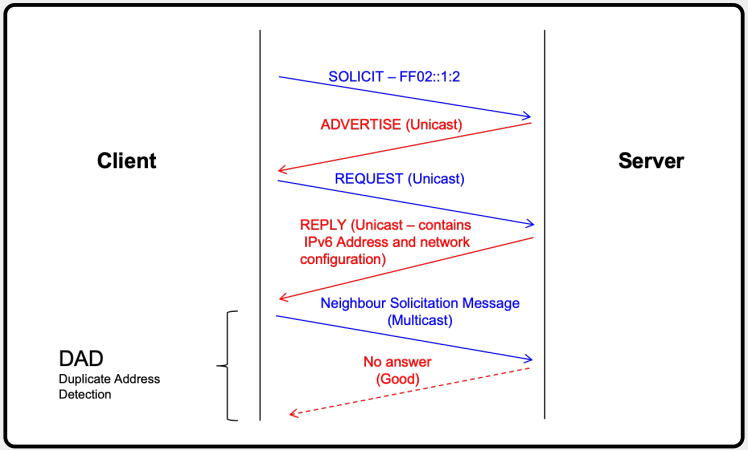

Figure 6: DORA becomes SARR

DHCPv6 Rapid Commit

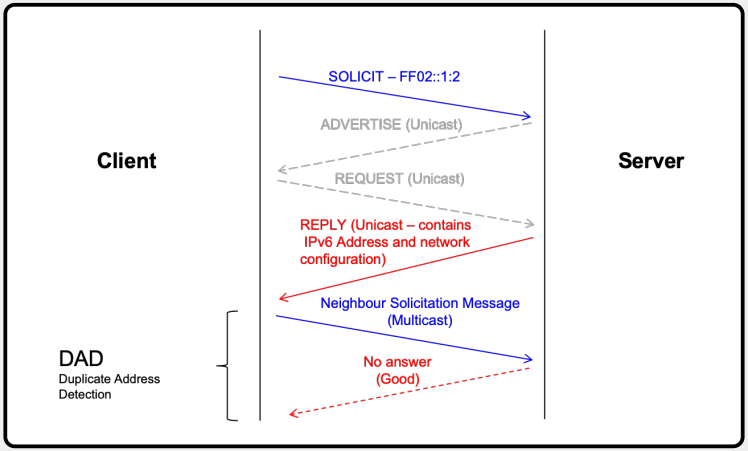

Figure 7: DHCPv6 Rapid Commit

DHCP Redundancy

Fail-Safe built into DHCP

- Client resends DHCPDISCOVER (or DHCPREQUEST) if unanswered
- Client keeps Address even without Service (T1 $\Rightarrow$ T2 $\Rightarrow$ Lease Expiration)
- longer Lease Times (causes other Side Effects)
- System-Level Redundancy (Cluster)
- NIC-Level Redundancy (Bonding)

DHCP Failover

- Internet Draft[1] but de-facto Standard
- Two Servers allocate same Address Pool (active/active)
- Failover Connections initiated over 647/TCP[2]
- Peers recover from an Outage safely and completely
- Relays need to be configured with both Server Addresses

[1] https://tools.ietf.org/html/draft-ietf-dhc-failover-12

[2] Port Numbers may vary

Ways in which Failover Peers lose Contact

- Servers can't differentiate between these Failures
  - Hardware or Software Problem
  - Local Network Failure
  - Network somewhere between Peers fails

DHCP Failover States

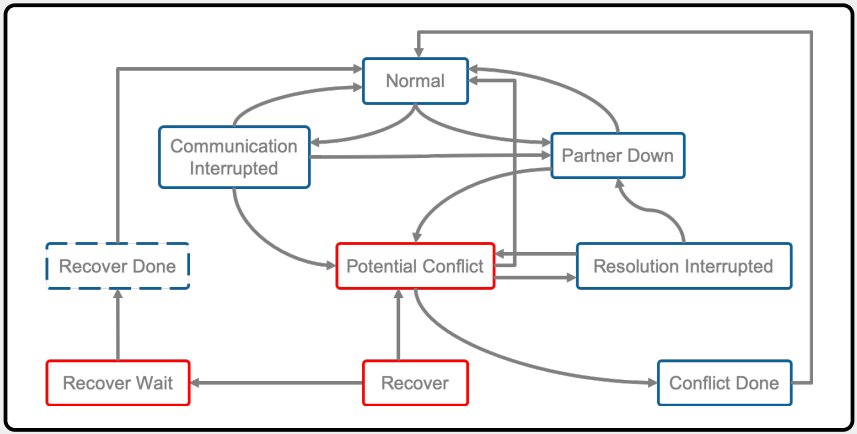

Figure 8: DHCP Failover States

DHCPv6 Redundancy Deployment Considerations (RFC 6853)

- Multiple unique, non-overlapping Pools simultaneously active and operational
- Multiple unique, non-overlapping Prefixes within the same Network
- One overlapping Prefix and Pool on multiple Servers

DHCPv6 Failover Protocol (RFC 8156)

- Independent Allocation
  - Pair of Servers configured with common Pool
  - Primary allocates even Addresses (least significant bit = 0)
  - Secondary allocated odd Addresses (least significant bit = 1)
  - Remaining Peer extends Renewals of Partner's Clients
- Proportional Allocation
  - Primary owns all delegable Prefixes
  - Secondary requests its Portion of delegable Prefixes from Primary
  - Failover Partners perform lazy Updates, (not immediately)
  - Binding Update (BNDUPD) used to send Changes to the Partner
  - Binding Acknowledgement (BNDREPLY) used for Confirmation of received Message

DHCPv6 Failover Messages

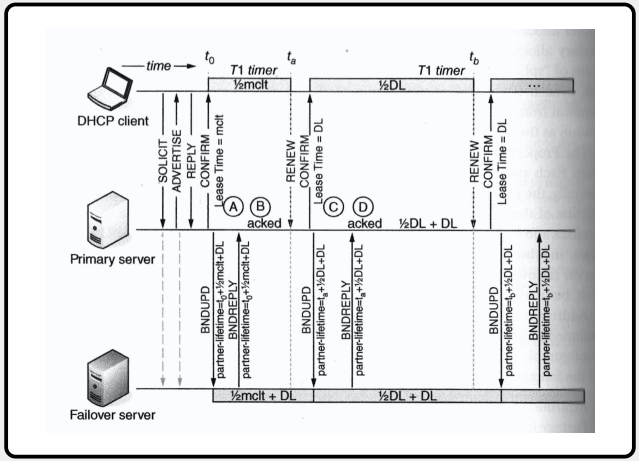

Figure 9: DHCPv6 Failover Messages

Influencers of DHCP

Long Lease Time

(+) Address Assignments are stable
(+) No Renumbering needed
(+) Low Packet Traffic
(+) Limited Impact of Server Outages

(-) Leases don't expire (depleted Pools)
(-) Changes to Option Values not propagated quickly
(-) Networks can't be renumbered automatically

Short Lease Time

(+) Changes propagate to Clients quickly
(+) Dynamic Pool Depletion is unlikely
(+) Client gets Address on new Subnets quickly

(-) Client's Address may change too frequently
(-) Leases Expire overnight
(-) Can cause heavy Load on Server
(-) Service must be highly available

Dynamic DNS

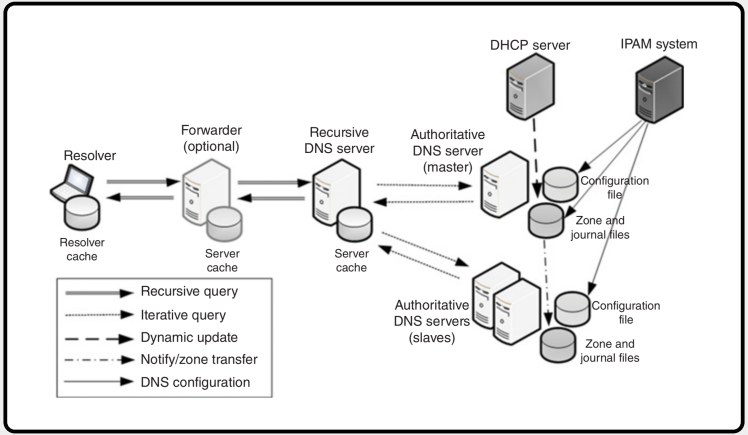

Figure 10: Dynamic DNS

Rogue DHCP Server

- Unauthorized DHCP Server set up by Attacker or by Accident
- Malicious DHCP Server on local Network replies faster
- Client can't authenticate DHCPOFFER

Unauthorized DHCP Client

- Attacker or uninvited Guest (unofficial device) obtains IP Address illegally
- MAC Address of valid Client gets spoofed by Attacker

DHCP Starvation (or Exhaustion)

- Many DHCPDISCOVER or DHCPREQUEST from malicious Client
- Could cause Denial of Service (DoS) due to no free Leases
- Also affects DNS through dynamic Updates by the DHCP Server
- dhcpstarv[1] and DHCPig[2]

[1] https://github.com/sgeto/dhcpstarv
[2] https://github.com/kamorin/DHCPig

Object Management API (omapi[1])

- ISC DHCP's Application Programming Interface (API)
- Query and manipulate Lease Data while the Server is running
- DHCP Server Objects: Lease, Host, Group, Control and Failover-State
- Get and set Attribute Values of Server Objects

[1] http://www.ipamworldwide.com/ipam/isc-dhcp-api.html

MAC Randomization[1]

- supported by iOS & Android
- MAC is dynamically changed for over-the-air Communications
- learn about Network Neighbours with random MAC
- real MAC used after successful Connection to Network
- optional lasting private MAC since iOS 14 & Android 10.0

[1] https://www.extremenetworks.com/extreme-networks-blog/wi-fi-mac-randomization-privacy-and-collateral-damage/

Hardening of DHCP

Disaster & Human Error Defences

- Geographic Provisioning of DHCP against natural & unnatural Disasters (earthquakes, hurricanes, floods, terrorist attacks, acts of war)
- Periodic User Trainings & Communication
- Roles & Responsibilities clearly enumerated and understood
- Change Control Meetings among relevant Stakeholders
- IPAM System to identify & correct potential Config. Errors
- Audit Logging to enable Review

Hardware & Operating System

- Physical Access (unplug, disconnect, console access)
- Updates & Patches for known Vulnerabilities (OS & Service)
- Protect Control Channel from unauthorized Access
- Permissions to Servers, Directories & Files containing DHCP Config.
- Monitoring of Logs (OS & Service)

DHCP Configuration

- Host Declaration (known & unknown clients)
- Class-based Address Allocation (user, vendor, vendor-specific, fingerprint)
- Zone Declaration for direct dynamic DNS Updates
- OMAPI Port & Key (if used)
- Monitoring of Configuration Changes

First-Hop Security

- DHCP Snooping validates DHCPOFFER/DHCPACK/DHCPNAK Messages from untrusted sources and filters invalid Messages
- DHCPv6 Guard blocks Reply/Advertisement Messages from unauthorized Servers and Relay Agents
- RA Guard blocks or rejects unwanted or rogue Router Advertisements

Authentication

- Authentication for DHCP Messages (RFC 3118)
- Authenticate Identity of other DHCP Participants
- Verify that Content of DHCP Message hasn't been changed during Delivery
- Backward Compatibility with existing Clients, Servers & Relay Agents
- Authentication via Kerberos, Token (plain text) or shared Secret (per client)

DHCPv6 Security

- HMAC-based[1] Authentication Option (DHCP realm, key ID, HMAC-MD5)
- DHCPv6 Security Considerations (RFC 8415 Section 22)
- IETF Draft for end-to-end Encryption of DHCPv6[2]

[1] Hash-based Message Authentication Code

[2] https://datatracker.ietf.org/doc/html/draft-ietf-dhc-sedhcpv6-21

Network Access Control (NAC)

- only authorized Clients on the Network
- Authentication based on Credentials or Certificates (802.1X)
- dynamic and static VLAN Deployments
- Guest Portal for external Devices

NetFlow

- De-facto Standard for Network Traffic Statistics
- Protocol for Layer-3 Devices to quantify the Traffic passing through
- Records huge Amount of Information
  (Who with whom? How long? Amount of Data? Protocol used?)
- Allows Troubleshooting, forensic Traffic Analysis, Intrusion Detection, etc.

DHCP Troubleshooting

Connectivity Problems

- Client is unable to communicate with DHCP Server at all (Firewall)
- DHCP Server is not receiving Client Messages (cf. listing 1)
- Client is not receiving Responses
- Relay is not configured for both Servers of Failover Association

```
1 tcpdump -i <interface> -nn -vvv '((port 67 or port 68) and (udp[38:4]= 0x<mac-address>))'
2 tcpdump -i eth0 -nn -vvv '((port 67 or port 68) and (udp[38:4]= 0xAC3FA470A6CE))'
```

Listing 1: tcpdump DHCP by MAC

Server Problems

- DHCP Service not started or crashed
- No available IP Addresses - “no free leases” (Pool Size, MDHCP)
- Server not configured for Client’s Network Segment (Zero Config. Networking)
- No Support for BOOTP Clients
- Server sends DHCPNAK Message
- More than one DHCP Server might exist (Rogue DHCP Servers)

Client Problems

- Missing Options from the DHCP Server (Parameter Request List)
- Incorrect Options from the DHCP Server (Inheritance)
- Very long Lease Time (Values not yet propagated)
- Client expect different Order of DHCP Options
- Client Identifier is not unique within administrative Domain
- Dual-Boot on Client's Systems
- Duplicate IP Addresses (static Clients)
- Client fails to get a reserved IP Address (MDHCP, MAC)
- Failure to acquire or renew a Lease

Thank you for your time.

honest Consulting

References

IP Address Management

by Michael Dooley, Timothy Rooney
Publisher: Wiley-IEEE Press
Release Date: March 2021
Pages: 640
ISBN-13: 978-1-119-69227-0

The DHCP Handbook

by Ralph Droms, Ted Lemon
Publisher: Sams Publishing
Release Date: November 2002
Pages: 588
ISBN-13: 978-0-672-32327-0

IPv6 Security

by Scott Hogg, Eric Vyncke
Publisher: Cisco Press
Release Date: December 2008
Pages: 540
ISBN-13: 978-1-587-05594-2