DHCP

Protocol workflow, attack vectors, and defensive architecture

Luca Campa

University of Klagenfurt – Introduction to Cybersecurity

Learning Goals

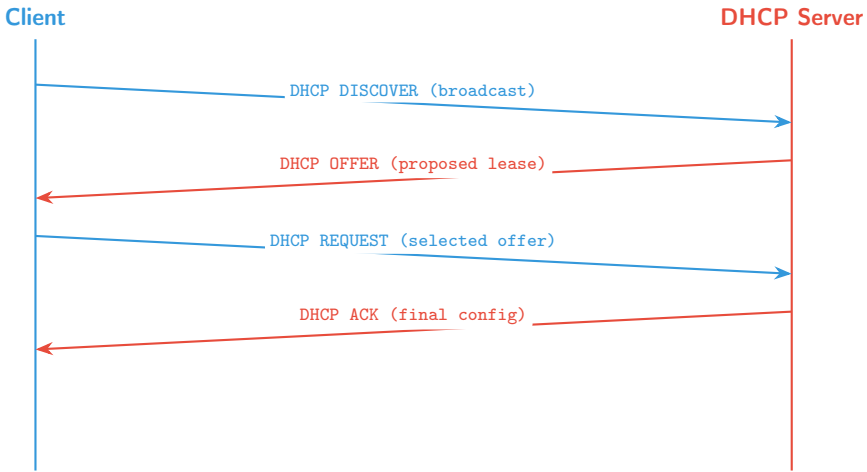
- Understand DHCP message flow and trust assumptions.
- Analyze major attacks: rogue DHCP, starvation, and option abuse.
- Explain impact on availability, confidentiality, and traffic integrity.
- Practical defenses: DHCP snooping, source guard, and monitoring strategies.

What DHCP Provides

- Automatic host configuration: IP address, subnet mask, gateway, DNS, lease time.
- Reduces manual errors and operational overhead.
- Built on UDP (client/server communication in broadcast domains).

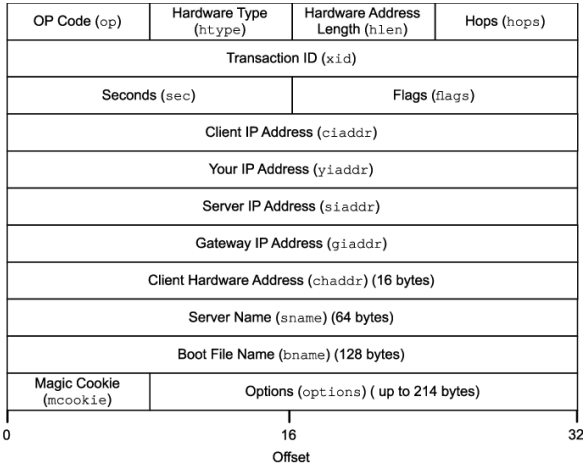
Weakness: classic DHCP has no strong built-in server authentication.

DHCP Exchange



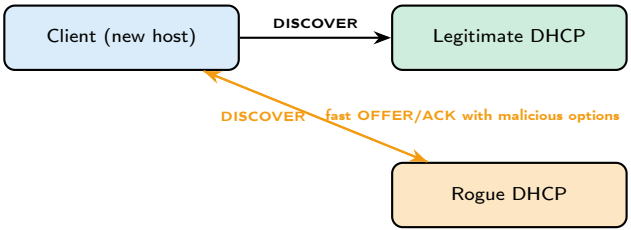
Note: Clients usually trust first valid offer/ack path unless network controls enforce legitimacy.

DHCP Packet Components (High Level)



Most attacks focus on abusing options and trust in who is allowed to answer.

Rogue DHCP Server Attack



Potential outcomes:

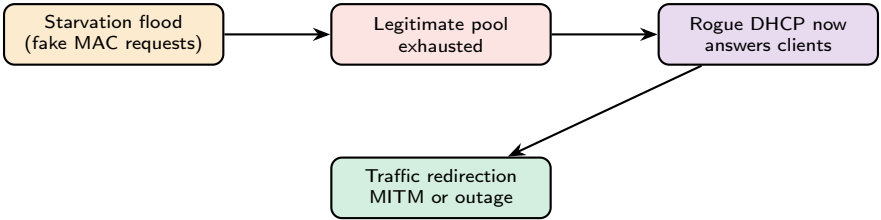
- malicious default gateway (traffic interception)
- rogue DNS (phishing, command-and-control redirection)
- blackhole routes (availability loss)

DHCP Starvation Attack

- Attacker sends many requests with spoofed/changing MAC addresses.
- DHCP pool is exhausted; legitimate clients fail to obtain leases.
- Often combined with rogue server for follow-on exploitation.

Impact: denial of service (issues in Availability)

DHCP Starvation and Rogue attacks combined



Option Abuse and Misconfiguration Risks

Malicious option (the field in the message format) values can:

- alter trust paths;
- preserve compromised settings (excessive lease duration);
- leak configuration across segments (poor relay-agent or VLAN scoping).

Note: a relay-agent is a network device (usually a router or Layer 3 switch) that forwards local DHCP broadcast requests from clients to a central DHCP server located on a different subnet.

DHCP Snooping (Switch-Level Defense)

- Mark switch ports as **trusted** (uplinks/authorized servers) or **untrusted** (access ports).
- Drop server-side DHCP replies from untrusted ports.
- Build binding tables (MAC, IP, VLAN, port, lease) for downstream protections.

Result: strong reduction of rogue DHCP risk in managed networks.

Using Snooping Bindings for More Protection

Control	Benefit
Dynamic ARP Inspection	Blocks ARP spoofing inconsistent with DHCP bindings
IP Source Guard	Prevents source IP/MAC spoofing at access ports
Port security + rate limits	Reduces starvation/flood effectiveness
VLAN segmentation	Limits DHCP incidents

DHCP Security Checklist

- Enable DHCP snooping on all access VLANs.
- Trust only uplink ports toward approved DHCP infrastructure.
- Apply per-port rate limits for DHCP requests.
- Monitor lease anomalies.
- Use secure DNS architecture (we'll see in the next lecture) to reduce impact of DNS-option abuse.
- In sensitive environments, **consider static addressing** for **critical systems**.

Possible DHCP Incident Indicators

- Increase in DISCOVER/REQUEST rates from single switch segments.
- Frequent duplicate IP conflicts after lease assignment.
- New/unknown DHCP server signatures in packet captures.
- Client complaints: “connected but no internet” or certificate errors due to DNS redirection.

CLI

Observe DHCP traffic (IPv4)

- Use tcpdump or Wireshark to filter for DHCP messages (UDP ports 67 and 68)
- `sudo tcpdump -n -i <interface> 'udp port 67 or udp port 68'`

Show ARP table and detect inconsistencies:

```
ip neighbor
```

Check assigned lease data (example path varies by distro and DHCP manager):

- dhclient:

  ```
  cat /var/lib/dhcp/dhclient.leases
  ```

- dhcpcd:

  ```
  /etc/dhcpcd.conf
  ```

Use only in authorized test environments.

References (Selected)

- RFC 2131: Dynamic Host Configuration Protocol.
- RFC 2132: DHCP Options and BOOTP Vendor Extensions.
- RFC 3046: DHCP Relay Agent Information Option.
- Vendor hardening guides for DHCP snooping and source guard.

Questions?