# End-to-End DHCP on Server with Router Relay (IPv4) + IPv6 (SLAAC/Stateful), DNS, SSH Hardening, ACL Mitigation, and DHCP Snooping in Cisco Packet Tracer

Overleaf-ready guide

August 15, 2025

## Contents



---

## 1 Lab Goal and Topology

**Goal:** Build a two-LAN Packet Tracer lab where the DHCP **Server** hands out IPv4 addresses to both LANs using `ip helper-address` on the Router. Add dual-stack IPv6 (SLAAC and

optional stateful DHCPv6 on the router), central **DNS** on the Server, **SSH** hardening on the Router, **DNS-filter ACLs**, and **DHCP snooping** on switches.

**Left LAN (g0/0/0)**
192.168.10.0/24, IPv6: 2001:DB8:10::/64

**Right LAN (g0/0/1)**
192.168.20.0/24, IPv6: 2001:DB8:20::/64

**Server (Right LAN)**
IPv4: 192.168.20.10, IPv6: 2001:DB8:20::10

**DNS**
Hosted on Server; name: `www.example.local`

**DHCPv4**
Hosted on Server for *both* LANs

**DHCPv6**
On Router (Packet Tracer router is reliable for DHCPv6)

**Quick ASCII Topology**

```
PC0 --- Left SW --- g0/0/0  R1  g0/0/1 --- Right SW --- Server + PCs
            192.168.10.0/24  |  192.168.20.0/24
            2001:DB8:10::/64 |  2001:DB8:20::/64
```

## 2 IP Plan

| Device/Network | Addressing |
|---|---|
| R1 g0/0/0 (Left) | IPv4 `192.168.10.1/24`, IPv6 `2001:DB8:10::1/64` |
| R1 g0/0/1 (Right) | IPv4 `192.168.20.1/24`, IPv6 `2001:DB8:20::1/64` |
| Server (Right) | IPv4 `192.168.20.10/24`, IPv6 `2001:DB8:20::10/64` |
| DNS | on Server (IPv4 & IPv6) |
| DHCPv4 Pools | `192.168.10.0/24` and `192.168.20.0/24` |

## 3 Router Base Configuration (Dual Stack)

```
! 1) Basic router setup
enable
conf t
 hostname R1
 no ip domain-lookup
 ip domain-name example.local
!
! 2) Left LAN
 interface g0/0/0
  description LEFT LAN
  ip address 192.168.10.1 255.255.255.0
  ipv6 address 2001:DB8:10::1/64
  no shutdown
!
! 3) Right LAN
 interface g0/0/1
```

```
  description RIGHT LAN
  ip address 192.168.20.1 255.255.255.0
  ipv6 address 2001:DB8:20::1/64
  no shutdown
!
! 4) Enable IPv6 routing
 ipv6 unicast-routing
end
wr
```

# 4 DHCPv4 on the Server (for Both LANs)

## 4.1 Server Static IP

On the Server (Right LAN) in Packet Tracer: **Desktop** → **IP Configuration**.

- IPv4 Address: `192.168.20.10`, Mask: `255.255.255.0`, Default GW: `192.168.20.1`
- IPv6 Address: `2001:DB8:20::10`, Prefix: `/64`, Default GW: `2001:DB8:20::1`

## 4.2 Enable DHCP Service and Create Pools

On the Server: **Services** → **DHCP** → **ON**. Create two pools:

### Right LAN Pool (192.168.20.0/24)

- Pool Name: `RIGHT-LAN`
- Default Gateway: `192.168.20.1`
- DNS Server: `192.168.20.10`
- Start IP: `192.168.20.21`
- Subnet Mask: `255.255.255.0`
- Max Users: `200`
- Domain Name: `example.local`

### Left LAN Pool (192.168.10.0/24)

- Pool Name: `LEFT-LAN`
- Default Gateway: `192.168.10.1`
- DNS Server: `192.168.20.10`
- Start IP: `192.168.10.21`
- Subnet Mask: `255.255.255.0`
- Max Users: `200`
- Domain Name: `example.local`

### 4.3 Relay DHCP from Left LAN using R1

Broadcasts from the left LAN must be relayed to the DHCP server in the right LAN. On R1:

```
enable
conf t
 interface g0/0/0
  ip helper-address 192.168.20.10
end
wr
```

*What does* ***ip helper-address*** *do?* By default it forwards several UDP services (including BOOTP/DHCP) as unicast to the helper IP. You can tighten this behavior (optional):

```
! Optional hardening: forward only DHCP/BOOTP and disable others
conf t
 no ip forward-protocol udp 37    ! time
 no ip forward-protocol udp 49    ! tacacs
 no ip forward-protocol udp 53    ! dns
 no ip forward-protocol udp 69    ! tftp
 no ip forward-protocol udp 137   ! netbios-ns
 no ip forward-protocol udp 138   ! netbios-dgm
end
wr
```

## 5 DNS on the Server

### 5.1 Enable DNS

On the Server: **Services** → **DNS** → **ON**.

### 5.2 Add Records

- A Record: `www.example.local` → `192.168.20.10`
- AAAA Record (optional): `www.example.local` → `2001:DB8:20::10`

## 6 IPv6 Addressing Methods

### 6.1 Stateless (SLAAC + DHCPv6 for other info)

Routers advertise prefixes; hosts auto-create addresses. Use the router-based pool for DNS/domain distribution.

```
conf t
 ipv6 dhcp pool V6-STATELESS
  dns-server 2001:DB8:20::10
  domain-name example.local
!
 interface g0/0/0
  ipv6 nd other-config-flag
  ipv6 dhcp server V6-STATELESS
!
 interface g0/0/1
  ipv6 nd other-config-flag
  ipv6 dhcp server V6-STATELESS
end
wr
```

On PCs: IPv6 set to *Auto Config* (do not tick DHCPv6 box in PT).

### 6.2 Stateful DHCPv6 (Full IPv6 via DHCPv6)

If you want full IPv6 from DHCPv6 (instead of SLAAC):

```
conf t
 ipv6 dhcp pool V6-STATEFUL-LEFT
  address prefix 2001:DB8:10::/64
  dns-server 2001:DB8:20::10
  domain-name example.local
!
 ipv6 dhcp pool V6-STATEFUL-RIGHT
  address prefix 2001:DB8:20::/64
  dns-server 2001:DB8:20::10
  domain-name example.local
!
 interface g0/0/0
  ipv6 nd managed-config-flag
  ipv6 dhcp server V6-STATEFUL-LEFT
!
 interface g0/0/1
  ipv6 nd managed-config-flag
  ipv6 dhcp server V6-STATEFUL-RIGHT
end
wr
```

On PCs: set IPv6 method to **DHCPv6**.

## 7 SSH Hardening on the Router

```
conf t
 username admin secret Pa55w0rd!
 ip ssh version 2
 crypto key generate rsa modulus 2048
 line vty 0 4
  login local
  transport input ssh
  exec-timeout 5 0
end
wr
```

*Notes:* Local user+secret, RSA 2048 keys, SSHv2 only, short idle timeout.

## 8 DNS Attack Mitigation with ACL

Apply an inbound ACL on both LAN interfaces to allow DNS only to the server and log other attempts.

```
conf t
 ip access-list extended DNS-FILTER
  permit udp any host 192.168.20.10 eq 53
  permit tcp any host 192.168.20.10 eq 53
  deny   udp any any eq 53 log
  deny   tcp any any eq 53 log
  permit ip any any
```

```
!
 interface g0/0/0
  ip access-group DNS-FILTER in
 interface g0/0/1
  ip access-group DNS-FILTER in
end
wr
```

## 9 DHCP Snooping on Switches

Enable snooping globally and on user VLAN(s). Trust only uplinks (to router) and the server-facing port.

**Left Switch**

```
conf t
 ip dhcp snooping
 ip dhcp snooping vlan 1
 ! trust the uplink to the router
 interface fa0/1
  ip dhcp snooping trust
end
wr
```

**Right Switch** Trust the port to the router and the **server** (since the server runs DHCPv4). Do *not* trust PC access ports.

```
conf t
 ip dhcp snooping
 ip dhcp snooping vlan 1
 interface fa0/1   ! uplink to router
  ip dhcp snooping trust
 interface fa0/2   ! port to Server
  ip dhcp snooping trust
end
wr
```

## 10 End-to-End Testing Checklist

Perform these in Packet Tracer after configs.

### A. IPv4 DHCP from Server

1. On **PC0** (Left LAN) `Desktop` → `IP Configuration` → `DHCP`.
2. Expect an IP in `192.168.10.21+`, Mask `/24`, GW `192.168.10.1`, DNS `192.168.20.10`.
3. On **PC1** (Right LAN) set `DHCP`. Expect `192.168.20.21+`, Mask `/24`, GW `192.168.20.1`, DNS `192.168.20.10`.

### B. DNS Resolution

1. On either PC: set DNS to `192.168.20.10` (auto if using DHCP).
2. Open Command Prompt: `ping www.example.local`

3. Optional (IPv6): `ping6 www.example.local`

### C. IPv6

1. For SLAAC: PC IPv6 set to Auto Config; verify a `2001:DB8:10::/64` or `2001:DB8:20::/64` address.
2. For Stateful: PC IPv6 set to DHCPv6; verify a lease from the correct pool.

### D. SSH

1. From a PC terminal: `ssh -l admin 192.168.20.1` (or `192.168.10.1`).
2. Login with the configured `admin` credentials; verify access and that telnet is refused.

### E. ACL Behavior

1. From a PC, try `nslookup` to any IP other than `192.168.20.10`; it should be blocked.
2. Check router logs for the `log` hits on `DNS-FILTER`.

## 11 Troubleshooting Tips

- **PCs not getting IP on Left LAN?** Ensure `ip helper-address 192.168.20.10` is on `g0/0/0`. Make sure DHCP service on the Server is ON and pools are correct.
- **DNS fails?** Confirm server has static IPs, DNS service is ON, and `www.example.local` A/AAAA records exist. Verify PCs have DNS set to `192.168.20.10`.
- **IPv6 not appearing?** For SLAAC, check `ipv6 unicast-routing` and RA flags (`other-config-flag` or `managed-config-flag`). For stateful, ensure pools are bound to the correct interfaces.
- **SSH not working?** Regenerate RSA keys after setting `ip domain-name`. Verify VTY lines allow only SSH and require local login.
- **DHCP Snooping drops?** Trust only uplinks and the DHCP server-facing port. End hosts should *not* be trusted.

## 12 Full Copy / Paste Scripts

### Router R1 (Base + IPv6 + ACL + SSH + Helper)

```
! Base + IPv6
conf t
 hostname R1
 no ip domain-lookup
 ip domain-name example.local
 interface g0/0/0
  description LEFT LAN
  ip address 192.168.10.1 255.255.255.0
  ipv6 address 2001:DB8:10::1/64
  no shutdown
 interface g0/0/1
  description RIGHT LAN
  ip address 192.168.20.1 255.255.255.0
  ipv6 address 2001:DB8:20::1/64
```

```
  no shutdown
 ipv6 unicast-routing
!
! DHCP relay to Server for Left LAN
 interface g0/0/0
  ip helper-address 192.168.20.10
!
! Optional: tighten helper to DHCP/BOOTP only
 no ip forward-protocol udp 37
 no ip forward-protocol udp 49
 no ip forward-protocol udp 53
 no ip forward-protocol udp 69
 no ip forward-protocol udp 137
 no ip forward-protocol udp 138
!
! SSH hardening
 username admin secret Pa55w0rd!
 ip ssh version 2
 crypto key generate rsa modulus 2048
 line vty 0 4
  login local
  transport input ssh
  exec-timeout 5 0
!
! DNS-filter ACL
 ip access-list extended DNS-FILTER
  permit udp any host 192.168.20.10 eq 53
  permit tcp any host 192.168.20.10 eq 53
  deny   udp any any eq 53 log
  deny   tcp any any eq 53 log
  permit ip any any
 interface g0/0/0
  ip access-group DNS-FILTER in
 interface g0/0/1
  ip access-group DNS-FILTER in
end
wr
```

## Router R1 (IPv6 DHCP options)

### Stateless (SLAAC + DHCPv6 for DNS)

```
conf t
 ipv6 dhcp pool V6-STATELESS
  dns-server 2001:DB8:20::10
  domain-name example.local
 interface g0/0/0
  ipv6 nd other-config-flag
  ipv6 dhcp server V6-STATELESS
 interface g0/0/1
  ipv6 nd other-config-flag
  ipv6 dhcp server V6-STATELESS
end
wr
```

### Stateful (Full DHCPv6)

```
conf t
 ipv6 dhcp pool V6-STATEFUL-LEFT
```

```
  address prefix 2001:DB8:10::/64
  dns-server 2001:DB8:20::10
  domain-name example.local
 ipv6 dhcp pool V6-STATEFUL-RIGHT
  address prefix 2001:DB8:20::/64
  dns-server 2001:DB8:20::10
  domain-name example.local
 interface g0/0/0
  ipv6 nd managed-config-flag
  ipv6 dhcp server V6-STATEFUL-LEFT
 interface g0/0/1
  ipv6 nd managed-config-flag
  ipv6 dhcp server V6-STATEFUL-RIGHT
end
wr
```

### Server (Right LAN)

#### Static IPs

- IPv4: `192.168.20.10/24`, GW `192.168.20.1`
- IPv6: `2001:DB8:20::10/64`, GW `2001:DB8:20::1`

#### DNS Service

- ON; add A: `www.example.local` $\rightarrow$ 192.168.20.10$AAAA(optional)$ : `www.example.local` $\rightarrow$ 2001 : $DB8$ : 20 :

#### DHCP Service (IPv4)

- Pool `RIGHT-LAN`: GW `192.168.20.1`, DNS `192.168.20.10`, Start `192.168.20.21`, Mask `255.255.255.0`, Domain `example.local`
- Pool `LEFT-LAN`: GW `192.168.10.1`, DNS `192.168.20.10`, Start `192.168.10.21`, Mask `255.255.255.0`, Domain `example.local`

### Switches

#### Left SW (trust uplink)

```
conf t
 ip dhcp snooping
 ip dhcp snooping vlan 1
 interface fa0/1
  ip dhcp snooping trust
end
wr
```

#### Right SW (trust uplink + server)

```
conf t
 ip dhcp snooping
 ip dhcp snooping vlan 1
 interface fa0/1  ! uplink to R1
  ip dhcp snooping trust
 interface fa0/2  ! to DHCP Server
  ip dhcp snooping trust
end
wr
```

## 13 How It All Fits Together (Step-by-Step Flow)

1. A PC on the Left LAN broadcasts DHCPDISCOVER. Because the server is on a different subnet, R1 (`g0/0/0`) uses `ip helper-address 192.168.20.10` to unicast-forward it to the server.
2. The Server's DHCP service selects the correct pool (LEFT-LAN) based on `giaddr` and replies with DHCPOFFER via R1 back to the client.
3. The PC receives an IPv4 lease (IP, mask, gateway, DNS, domain). On the Right LAN, the process is simpler (same subnet as server).
4. DNS queries from clients are allowed only to the server by the `DNS-FILTER` ACL; other DNS attempts are denied and logged.
5. For IPv6, either **SLAAC**+DHCPv6 (other info) or **stateful DHCPv6** is provided by the router, depending on the chosen flags and pools.
6. SSH access to R1 is secured: only SSHv2, local authentication, 2048-bit RSA, and short idle timeout.
7. DHCP Snooping prevents rogue DHCP servers; only the router uplinks and the legitimate server port are trusted.

## ★ You Are Ready to Test

Follow the *End-to-End Testing Checklist*; you should see working DHCPv4 from the Server across both LANs, DNS resolution, IPv6 addressing as configured, SSH-only management, and ACL enforcement.

**Tip:** If you want, you can add NTP and Syslog for richer logs and time-stamped ACL hits.