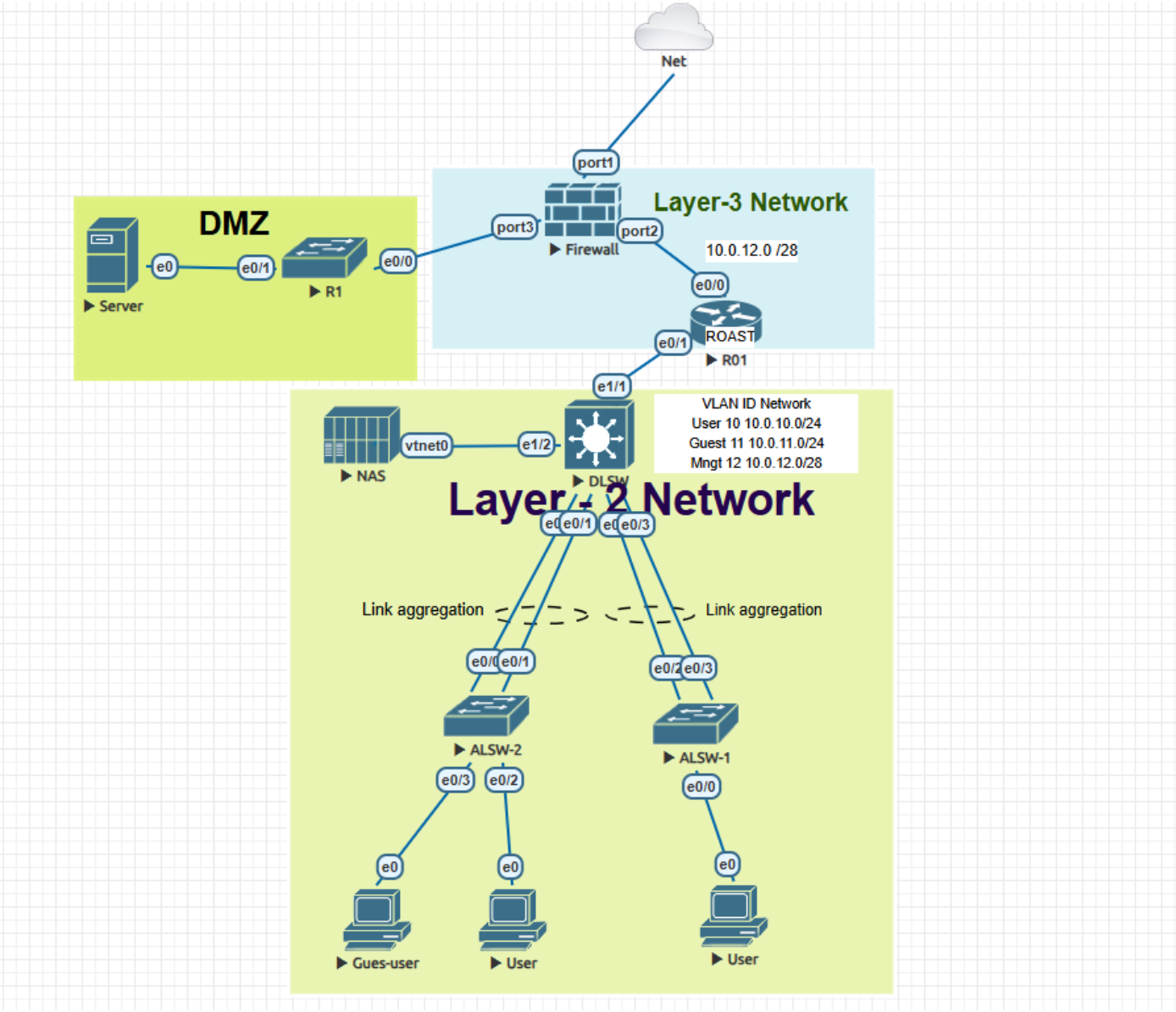


This enterprise network architecture is designed to ensure both scalability and security. The purpose of this emulation is to penetrate mitigate two of the most common cyber threats within the network, which often arise due to inadequate security measures and social engineering attacks.

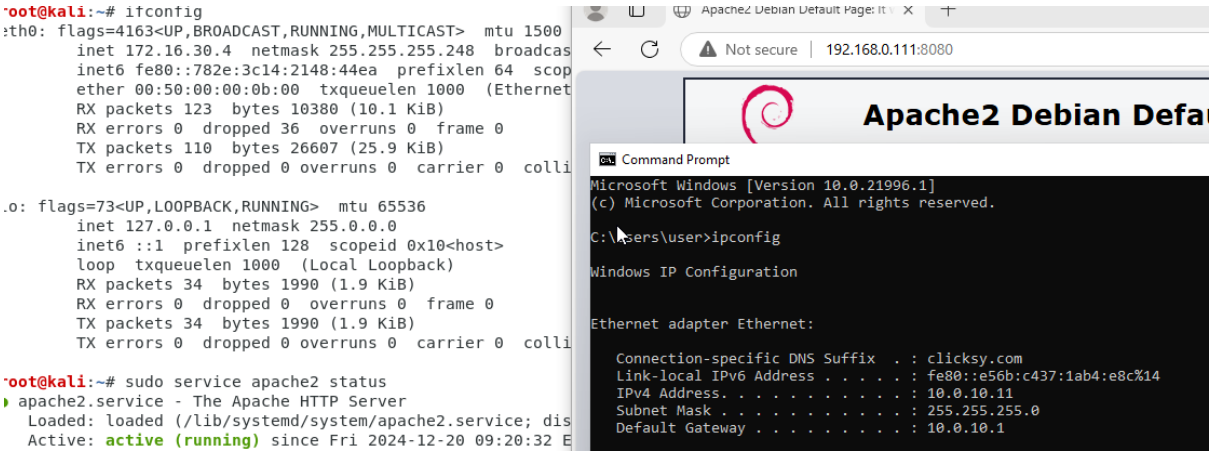
Next Generation firewall

Interface configuration

```
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.0.111 255.255.255.0
        set allowaccess https ssh http fgfm
        set type physical
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 192.168.1.1 255.255.255.252
        set allowaccess ping https ssh fgfm ftm
        set type physical
        set snmp-index 2
    next
    edit "port3"
        set vdom "root"
        set ip 172.16.30.1 255.255.255.248
        set allowaccess ping https ssh fgfm
        set type physical
        set alias "dmz"
        set snmp-index 3
    next
```

DMZ:

The DMZ is isolated from the internal network to enhance security and provide controlled access to external users.



Layer-3 Network:

Router R01 connects to the Layer-3 network, providing routing between subnets and access to the Layer-2 network.

```
R01(config-if)#do show ip int br
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            192.168.1.2     YES NVRAM  up                    up
Ethernet0/1            unassigned      YES NVRAM  up                    up
Ethernet0/1.10         10.0.10.1       YES NVRAM  up                    up
Ethernet0/1.11         10.0.11.1       YES NVRAM  up                    up
Ethernet0/1.12         10.0.12.1       YES NVRAM  up                    up
Ethernet0/2            unassigned      YES NVRAM  administratively down down
Ethernet0/3            unassigned      YES NVRAM  administratively down down
```

Layer-2 Network:

Contains a core distribution switch (DLSW) connecting to access layer switches (ALSW-1 and ALSW-2).

VLANs

```
DLSW#show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/3
10   user                             active
11   guest                            active
12   mngt                             active    Et1/0, Et1/2
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
```

VTP

```
DLSW#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : clicksy.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc00.3000
Configuration last modified by 0.0.0.0 at 12-18-24 13:42:37
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 8
Configuration Revision            : 7
MD5 digest                        : 0x65 0xA8 0xB8 0x21 0xB4 0xDD 0x2D 0x14
                                    0x64 0xFC 0x20 0xA3 0x34 0x6F 0xDC 0xB1
```

```
ALSW1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : clicksy.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc00.4000
Configuration last modified by 0.0.0.0 at 12-18-24 13:42:37

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 8
Configuration Revision            : 7
MD5 digest                        : 0x65 0xA8 0xB8 0x21 0xB4 0xDD 0x2D 0x14
                                    0x64 0xFC 0x20 0xA3 0x34 0x6F 0xDC 0xB1
```

Port Aggregation

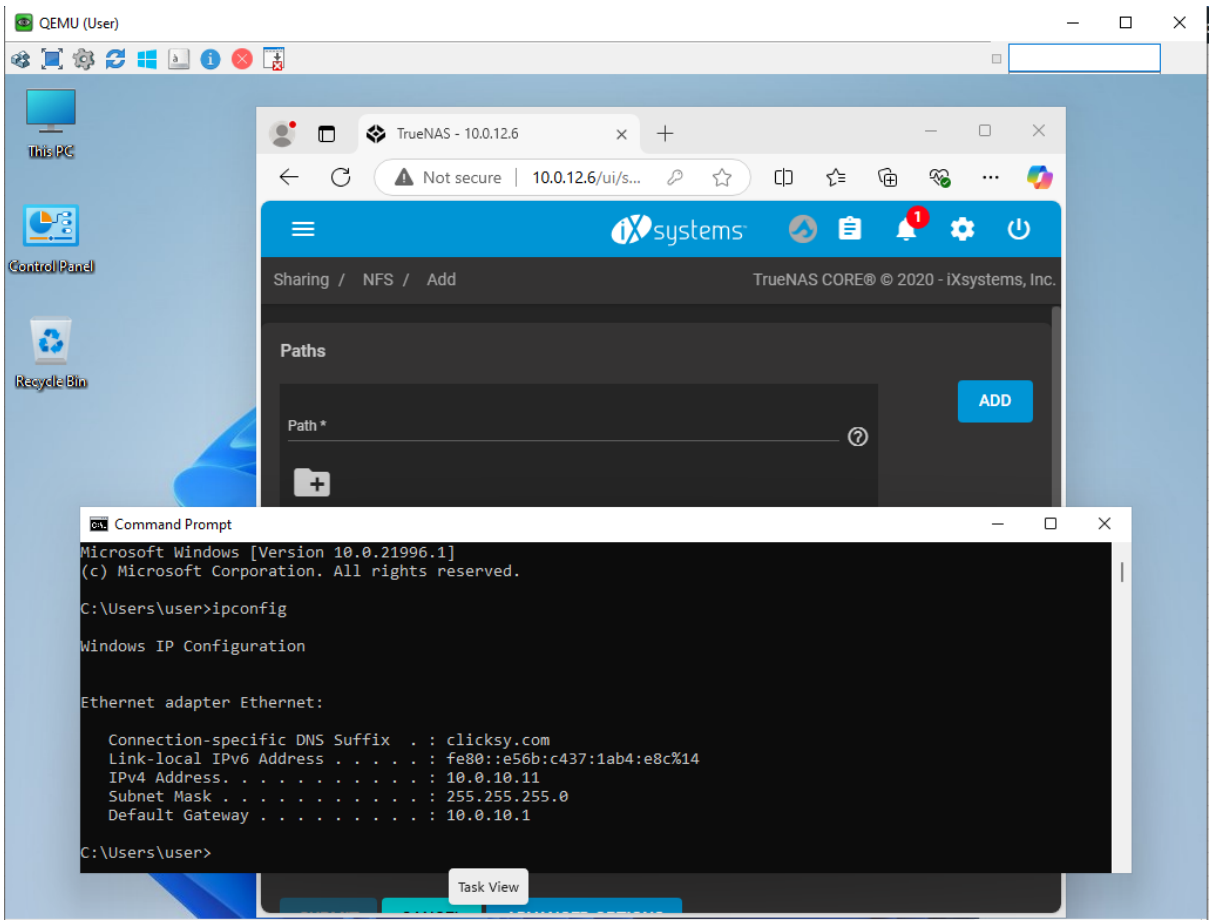
```
DLSW#show etherchannel sum
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Et0/0(P)    Et0/1(P)
2      Po2(SU)         LACP      Et0/2(P)    Et0/3(P)
```

Network Attached Storage (NAS):



Connected to the DLSW on vtnet0 for centralized storage and data sharing.

DHCP Binding

```
R01#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.0.10.11          0150.0000.0a00.00       Dec 21 2024 12:57 PM    Automatic
10.0.11.101         0150.0000.0800.00       Dec 21 2024 12:57 PM    Automatic
10.0.11.102         0100.5000.0009.00       Dec 21 2024 12:57 PM    Automatic
```

MAC Tables

```
ALSW1#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    5000.000a.0000    DYNAMIC     Et0/2
  10    aabb.cc00.6010    DYNAMIC     Et0/1
Total Mac Addresses for this criterion: 2
```

```
ALSW2#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    5000.000a.0000    DYNAMIC     Et0/2
Total Mac Addresses for this criterion: 1
```

Scenario -1 described before attack

Two guest computers are connected with the network one of guest suspicious

Guest – User -1 IP address

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.11.102  netmask 255.255.255.0  broadcast 10.0.11.255
        inet6 fe80::f662:b598:b315:978  prefixlen 64  scopeid 0x20<link>
        ether 00:50:00:00:09:00  txqueuelen 1000  (Ethernet)
        RX packets 26  bytes 2561 (2.5 KiB)
        RX errors 0  dropped 20  overruns 0  frame 0
        TX packets 30  bytes 3036 (2.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Guest-User-2 IP address

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : clicksy.com
   Link-local IPv6 Address . . . . . : fe80::7050:f430:bd8a:6504%4
   IPv4 Address. . . . . . . . . . . : 10.0.11.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.11.1
```

Router

```
R01#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.0.11.102         0100.5000.0009.00       Dec 21 2024 08:05 PM    Automatic
10.0.11.103         0150.0000.0c00.00       Dec 21 2024 08:02 PM    Automatic
```

Generate attack

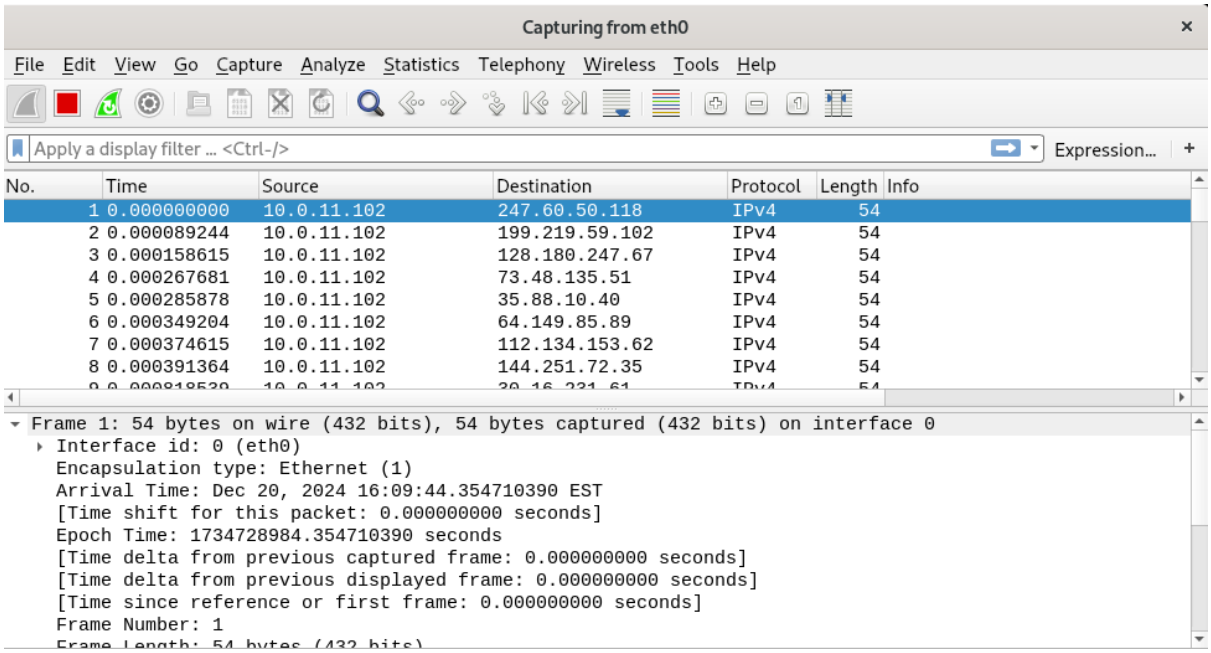
Rogue DCHP server is an unauthorized or malicious DHCP server on a network. It can cause significant issues by distributing incorrect IP configuration settings to devices.

Router assigned all IP address to fake MAC

```
R01#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.0.11.101         0a1d.8713.0245          Dec 20 2024 08:45 PM    Automatic
10.0.11.102         0100.5000.0009.00       Dec 21 2024 08:05 PM    Automatic
10.0.11.103         0150.0000.0c00.00       Dec 21 2024 08:02 PM    Automatic
10.0.11.104         68dc.090b.eca5          Dec 20 2024 08:45 PM    Automatic
10.0.11.105         8a29.632e.aa21          Dec 20 2024 08:45 PM    Automatic
10.0.11.106         605d.1f1e.07a1          Dec 20 2024 08:45 PM    Automatic
10.0.11.107         e25f.773c.d9f3          Dec 20 2024 08:45 PM    Automatic
10.0.11.108         24e5.b974.0712          Dec 20 2024 08:45 PM    Automatic
10.0.11.109         100c.8162.e83d          Dec 20 2024 08:45 PM    Automatic
10.0.11.110         2676.9675.ece2          Dec 20 2024 08:45 PM    Automatic
10.0.11.111         fe3c.8b1d.5b87          Dec 20 2024 08:45 PM    Automatic
10.0.11.112         22f9.d102.1a8b          Dec 20 2024 08:45 PM    Automatic
```

MAC Flooding attack

A single IP address generating a large number of MAC addresses can cause a MAC address table overflow, leading to a MAC address storm on the switch.



Mitigating Rogue DHCP Servers

1. Enable DHCP spoofing and port security layer 2 network
2. Dynamic ARP Inspection (DAI) and blocking traffic from unauthorised mac address

Recommendation

Based on my experience, social engineering plays a significant role in such incidents. In most cases, guests attempt to convince employees to grant them access to the user network, often citing reasons like slow internet connectivity or other issues. It is highly recommended never to compromise any security measures under any circumstances, regardless of the situation.