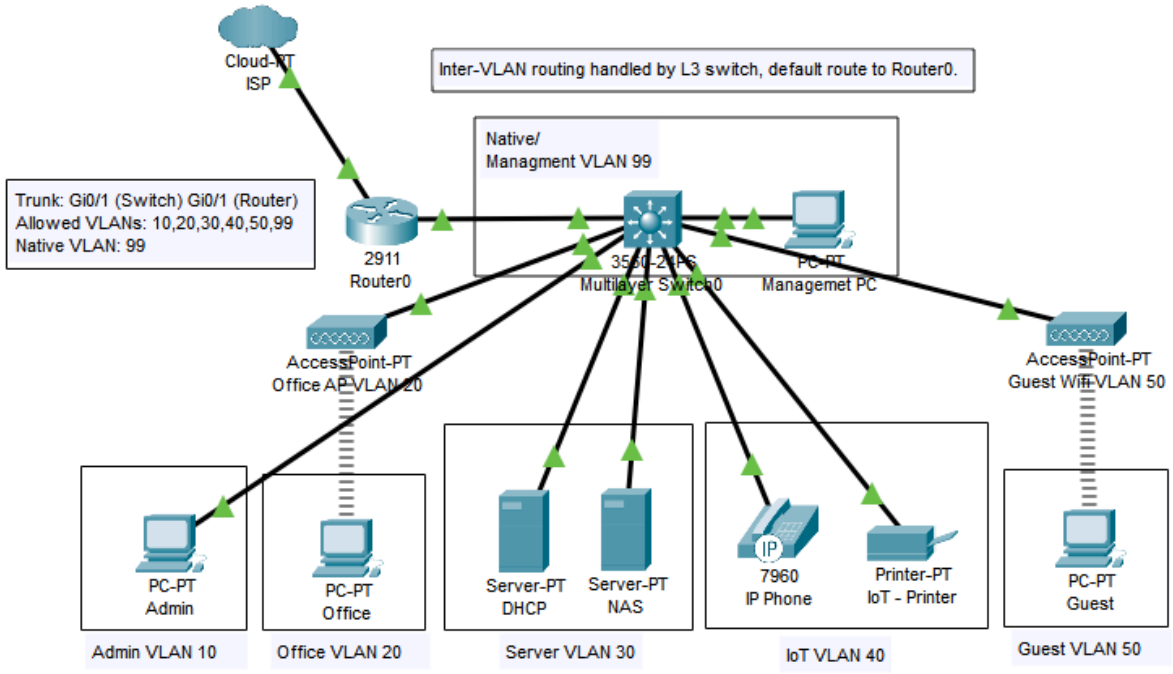
Secure Multi VLAN Small Business Network

Jacob Lau

I designed and deployed a secure multi VLAN small office network using a Cisco 2911 router and 3560 multilayer switch in Packet Tracer. The network supports separate security zones for admin, office, servers, IoT, guests, and management. Inter VLAN routing is handled on the L3 switch through SVIs, with DHCP delivered centrally via helper addresses and NAT configured at the router edge. Extended ACLs enforce strict segmentation to prevent lateral movement between VLANs, while device hardening improves management security. This project demonstrates practical experience in network design, routing, DHCP relay, VLAN segmentation, ACL security, and infrastructure hardening.

A segmented multi VLAN network with ACL enforcement, DHCP relay, NAT, and hardening.



IP Addressing Plan

This table documents all static and DHCP assigned IPs for each VLAN.

VLAN	Purpose	Subnet	Gateway	Device	IP Address
10	Admin	10.10.10.0 /24	10.10.10.1	Admin PC	10.10.10.10
20	Office	10.10.20.0 /24	10.10.20.1	Office WiFi Client (example)	10.10.20.100 (DHCP)
30	Server	10.10.30.0 /24	10.10.30.1	DHCP Server	10.10.30.10
				NAS Server	10.10.30.20
40	IoT	10.10.40.0 /24	10.10.40.1	IoT Printer	10.10.40.30
				IoT Device (camera placeholder)	10.10.40.10 (optional)
50	Guest	10.10.50.0 /24	10.10.50.1	Guest WiFi Client	10.10.50.100 (DHCP)
99	Management	10.10.99.0 /24	10.10.99.1	Management PC	10.10.99.100
				AP Management Interface	10.10.99.20
—	Router External	200.200.200.0 /24	N/A	Router G0/0	200.200.200.2
—	Router Internal	varies per subinterface	varies	Router G0/1.x	10.10.x.254

VLAN Security policies

VLAN 10 – Admin

- Full access to all internal VLANs and devices
- Unrestricted for management, troubleshooting, and maintenance
- Trusted subnet

VLAN 20 – Office

- Access to Server VLAN for business services
- Internet access through NAT
- No access to Admin, IoT, or Guest VLANs
- Standard employee subnet

VLAN 30 – Server

- Central services: DHCP, NAS, application servers
- Accessible from all VLANs based on role
- Restricted from initiating outbound sessions except responses
- High trust

VLAN 40 – IoT

- Access to Server VLAN (logging, storage)
- Internet access
- Blocked from Admin, Office, and Guest VLANs
- Untrusted subnet

VLAN 50 – Guest

- Internet access only
- Fully isolated from all internal VLANs
- Zero trust zone

VLAN 99 – Management

- Used for administration of switch, router, and APs
- Not accessible from Guest, IoT, or Office VLANs
- Restricted to Admin subnet

ACL Security Model

ACLs are applied inbound on each SVI to enforce segmentation boundaries.

ADMIN_IN

- permit ip any any
- Admin has full access to all resources.

OFFICE_IN

- Deny Office → Admin
- Deny Office → IoT
- Deny Office → Guest
- Permit Office → Server
- Permit Office → Internet

SERVER_IN

- Permit Admin/Office/IoT/Guest → Server
- Permit Server → any (responses)

IOT_IN

- Deny IoT → Admin
- Deny IoT → Office
- Deny IoT → Guest
- Permit IoT → Server
- Permit IoT → Internet

GUEST_IN

- Deny Guest → Admin
- Deny Guest → Office
- Deny Guest → Server
- Deny Guest → IoT
- Permit Guest → Internet

Configuration Excerpts

Only key configuration portions are shown here for clarity.

```
vlan 10
 name Admin
vlan 20
 name Office
vlan 30
 name Server
vlan 40
 name IoT
vlan 50
 name Guest
vlan 99
 name Management

interface vlan 10
 ip address 10.10.10.1 255.255.255.0
 ip access-group ADMIN_IN in

interface vlan 20
 ip address 10.10.20.1 255.255.255.0
 ip access-group OFFICE_IN in

interface vlan 30
 ip address 10.10.30.1 255.255.255.0
 ip access-group SERVER_IN in

interface vlan 40
 ip address 10.10.40.1 255.255.255.0
 ip access-group IOT_IN in

interface vlan 50
 ip address 10.10.50.1 255.255.255.0
 ip access-group GUEST_IN in

interface vlan 99
 ip address 10.10.99.1 255.255.255.0
```

DHCP Relay

```
interface vlan 10
 ip helper-address 10.10.30.10
interface vlan 20
 ip helper-address 10.10.30.10
interface vlan 40
 ip helper-address 10.10.30.10
interface vlan 50
 ip helper-address 10.10.30.10
interface vlan 99
 ip helper-address 10.10.30.10
```

Router Subinterfaces

```
interface g0/1.10
 encapsulation dot1Q 10
 ip address 10.10.10.254 255.255.255.0

interface g0/1.20
 encapsulation dot1Q 20
 ip address 10.10.20.254 255.255.255.0

interface g0/1.30
 encapsulation dot1Q 30
 ip address 10.10.30.254 255.255.255.0

interface g0/1.40
 encapsulation dot1Q 40
 ip address 10.10.40.254 255.255.255.0

interface g0/1.50
 encapsulation dot1Q 50
 ip address 10.10.50.254 255.255.255.0

interface g0/1.99
 encapsulation dot1Q 99
 ip address 10.10.99.254 255.255.255.0
```

NAT Configuration

```
interface g0/0
 ip nat outside
interface g0/1
 ip nat inside

access-list 1 permit 10.10.0.0 0.0.255.255
ip nat inside source list 1 interface g0/0 overload
```

Switch/Router Hardening

```
no ip http server
no ip http secure-server
ip ssh version 2
line vty 0 4
 transport input ssh
 login local
```

ACL Verification

Deny counters verify that segmentation is functioning as expected.

```
SW-Branch#show access-lists
Extended IP access list ADMIN_IN
    10 permit ip any any (12 match(es))
Extended IP access list OFFICE_IN
    5 permit ip 10.10.10.0 0.0.0.255 any
    10 deny ip 10.10.20.0 0.0.0.255 10.10.10.0 0.0.0.255 (4 match(es))
    20 deny ip 10.10.20.0 0.0.0.255 10.10.40.0 0.0.0.255
    30 deny ip 10.10.20.0 0.0.0.255 10.10.50.0 0.0.0.255
    40 permit ip 10.10.20.0 0.0.0.255 10.10.30.0 0.0.0.255 (4 match(es))
    50 permit ip 10.10.20.0 0.0.0.255 any
Extended IP access list IOT_IN
    5 permit ip 10.10.10.0 0.0.0.255 any
    10 deny ip 10.10.40.0 0.0.0.255 10.10.10.0 0.0.0.255
    20 deny ip 10.10.40.0 0.0.0.255 10.10.20.0 0.0.0.255
    30 deny ip 10.10.40.0 0.0.0.255 10.10.50.0 0.0.0.255
    40 permit ip 10.10.40.0 0.0.0.255 10.10.30.0 0.0.0.255
    50 permit ip 10.10.40.0 0.0.0.255 any
Extended IP access list GUEST_IN
    5 permit ip 10.10.10.0 0.0.0.255 any
    10 deny ip 10.10.50.0 0.0.0.255 10.10.10.0 0.0.0.255
    20 deny ip 10.10.50.0 0.0.0.255 10.10.20.0 0.0.0.255
    30 deny ip 10.10.50.0 0.0.0.255 10.10.30.0 0.0.0.255
    40 deny ip 10.10.50.0 0.0.0.255 10.10.40.0 0.0.0.255
    50 permit ip 10.10.50.0 0.0.0.255 any
Extended IP access list SERVER_IN
    10 permit ip any 10.10.30.0 0.0.0.255
    20 permit ip 10.10.30.0 0.0.0.255 any (12 match(es))

SW-Branch#
```

IP Interface

This confirms DHCP relay, SVI configuration, and interface status.

```
SW-Branch#show ip int b
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES unset  administratively down down
FastEthernet0/2        unassigned      YES unset  administratively down down
FastEthernet0/3        unassigned      YES unset  administratively down down
FastEthernet0/4        unassigned      YES unset  administratively down down
FastEthernet0/5        unassigned      YES unset  administratively down down
FastEthernet0/6        unassigned      YES unset  administratively down down
FastEthernet0/7        unassigned      YES unset  administratively down down
FastEthernet0/8        unassigned      YES unset  administratively down down
FastEthernet0/9        unassigned      YES unset  administratively down down
FastEthernet0/10       unassigned      YES unset  administratively down down
FastEthernet0/11       unassigned      YES unset  administratively down down
FastEthernet0/12       unassigned      YES unset  administratively down down
FastEthernet0/13       unassigned      YES unset  administratively down down
FastEthernet0/14       unassigned      YES unset  up                    up
FastEthernet0/15       unassigned      YES unset  up                    up
FastEthernet0/16       unassigned      YES unset  administratively down down
FastEthernet0/17       unassigned      YES unset  administratively down down
FastEthernet0/18       unassigned      YES unset  up                    up
FastEthernet0/19       unassigned      YES unset  up                    up
FastEthernet0/20       unassigned      YES unset  administratively down down
FastEthernet0/21       unassigned      YES unset  administratively down down
FastEthernet0/22       unassigned      YES unset  up                    up
FastEthernet0/23       unassigned      YES unset  up                    up
FastEthernet0/24       unassigned      YES unset  up                    up
GigabitEthernet0/1     unassigned      YES unset  up                    up
GigabitEthernet0/2     unassigned      YES unset  up                    up
Vlan1                  unassigned      YES unset  administratively down down
Vlan10                 10.10.10.1      YES manual up                    up
Vlan20                 10.10.20.1      YES manual up                    up
Vlan30                 10.10.30.1      YES manual up                    up
Vlan40                 10.10.40.1      YES manual up                    up
Vlan50                 10.10.50.1      YES manual up                    up
Vlan99                 10.10.99.1      YES manual up                    up
SW-Branch#
```

DHCP Bindings

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Addre
VLAN99	10.10.99.1	1.1.1.1	10.10.99...	255.255....	100	0.0.0.0	0.0.0.0
VLAN50	10.10.50.1	1.1.1.1	10.10.50...	255.255....	100	0.0.0.0	0.0.0.0
VLAN40	10.10.40.1	1.1.1.1	10.10.40...	255.255....	100	0.0.0.0	0.0.0.0
VLAN30	10.10.30.1	1.1.1.1	10.10.30...	255.255....	100	0.0.0.0	0.0.0.0
VLAN20	10.10.20.1	1.1.1.1	10.10.20...	255.255....	100	0.0.0.0	0.0.0.0
VLAN10	10.10.10.1	1.1.1.1	10.10.10...	255.255....	100	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	10.10.30.0	255.255....	512	0.0.0.0	0.0.0.0