ISP Integration & Network Configuration Report

Cisco Packet Tracer – Static Routing Lab

Field	Details
Project File	Static Routing.pkt
Simulator	Cisco Packet Tracer
Topology	Sydney LAN + Melbourne LAN + ISP Router
Report Date	25 May 2026
Author	Network Administrator
Classification	Internal

1. Executive Summary

This report documents the process of integrating an Internet Service Provider (ISP) router into an existing dual-site Cisco network environment simulated in Cisco Packet Tracer. The configuration covers ISP router setup, WAN link establishment, default static routing, NAT/PAT configuration, and connectivity verification between the Sydney and Melbourne sites via the ISP.

Key outcomes achieved:

- ISP Router configured with GigabitEthernet0/0 WAN interface and loopback 0 for simulated internet reachability
- Sydney Router linked to ISP via /30 subnet (8.8.8.0/30) with a default static route
- NAT/PAT configured on Sydney Router to translate internal RFC 1918 addresses to the public WAN IP

- Successful ICMP connectivity confirmed from Sydney Router to ISP loopback (9.9.9.9) and vice versa
- ISP Router configured with return routes to reach the Sydney inside networks

2. Network Topology Overview

The lab topology consists of three routing devices interconnected to simulate a typical enterprise WAN environment:

Device	Model	Role	Key Interfaces
Switch Sydney	2960-24TT	Layer 2 Access Switch	Fa0/1, Fa0/2, Fa0/3
Router Sydney	2911	Site Gateway / NAT Router	Gig0/0, Gig0/1, Gig0/2
ISP Router	2911	Internet Service Provider	Gig0/0, Loopback0
Router Melbourne	2911	Remote Site Gateway	Gig0/0, Gig0/1
Switch Melbourne	2960-24TT	Layer 2 Access Switch	Fa0/1, Fa0/2, Fa0/3
Sydney PC1	PC-PT	End Host	Fa0
Sydney PC2	PC-PT	End Host	Fa0
Melbourne PC1	PC-PT	End Host	Fa0
Melbourne PC2	PC-PT	End Host	Fa0

The Sydney Router connects to the ISP Router via its Gig0/2 interface using a dedicated /30 WAN subnet. The Melbourne Router connects to the Sydney Router via Gig0/1 for inter-site connectivity. The dashed line between Router Sydney (Gig0/1) and Router Melbourne (Gig0/1) represents the WAN link between the two sites.

3. IP Addressing Scheme

The following IP address plan was implemented across all devices:

Network / Segment	Subnet	Device Interface	IP Address
Sydney LAN 1	192.168.10.0/24	Router Sydney Gig0/0.10	192.168.10.1
Sydney LAN 2	192.168.20.0/24	Router Sydney Gig0/0.20	192.168.20.1
Sydney–Melbourne WAN	10.0.0.0/30	Router Sydney Gig0/1	10.0.0.1
Sydney–ISP WAN	8.8.8.0/30	Router Sydney Gig0/2	8.8.8.1
Sydney–ISP WAN	8.8.8.0/30	ISP Router Gig0/0	8.8.8.2

Network / Segment	Subnet	Device Interface	IP Address
ISP Loopback (Internet Sim)	9.9.9.9/32	ISP Router Loopback0	9.9.9.9
Melbourne LAN 1	192.168.30.0/24	Router Melbourne Gig0/0 sub	192.168.30.1
Melbourne LAN 2	192.168.40.0/24	Router Melbourne Gig0/0 sub	192.168.40.1

4. Configuration Steps

4.1 ISP Router – Interface & Loopback Configuration

The ISP Router was configured with its GigabitEthernet0/0 interface as the customer-facing WAN port, and a loopback interface to simulate a public internet address (9.9.9.9) reachable from the Sydney site.

```
Router> en
Router# conf t
Router(config)# int g0/0
Router(config-if)# ip address 8.8.8.2 255.255.255.252
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface loopback 0
Router(config-if)# ip address 9.9.9.9 255.255.255.255
Router(config-if)# exit
```

The loopback interface came up automatically once configured. The GigabitEthernet0/0 interface transitioned to the 'up/up' state upon issuing 'no shutdown'.

4.2 Router Sydney – WAN Interface Configuration

Sydney Router's Gig0/2 interface was configured to connect to the ISP using the other end of the /30 WAN link. A default static route was then added pointing all unknown traffic toward the ISP gateway.

```
Router> en
Router# conf t
Router(config)# int g0/2
Router(config-if)# ip address 8.8.8.1 255.255.255.252
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# ip route 0.0.0.0 0.0.0.0 8.8.8.2
Router(config)# exit
```

Verification: After applying the default route, a ping to 9.9.9.9 from Router Sydney yielded a success rate of 80% (4/5 packets), confirming WAN reachability. The first packet drop is expected due to ARP resolution.

4.3 Router Sydney – NAT/PAT Configuration

Network Address Translation with Port Address Translation (PAT/Overload) was configured to allow internal hosts across all subnets to reach the ISP using the single public IP 8.8.8.1 on Gig0/2. OSPF was also enabled to propagate the default route into the routing domain.

```
Router(config)# router ospf 1
Router(config-router)# default-information originate
Router(config-router)# exit

! Mark inside NAT interfaces
Router(config)# int g0/0.10
Router(config-subif)# ip nat inside
Router(config-subif)# exit
Router(config)# int g0/0.20
Router(config-subif)# ip nat inside
Router(config-subif)# exit
Router(config)# int g0/1
Router(config-if)# ip nat inside
Router(config-if)# exit

! Mark outside NAT interface
Router(config)# int g0/2
Router(config-if)# ip nat outside
Router(config-if)# exit

! Define ACL for inside networks
Router(config)# access-list 1 permit 192.168.10.0 0.0.0.255
Router(config)# access-list 1 permit 192.168.20.0 0.0.0.255
Router(config)# access-list 1 permit 10.0.0.0 0.0.0.3
Router(config)# access-list 1 permit 192.168.30.0 0.0.0.255
Router(config)# access-list 1 permit 192.168.40.0 0.0.0.255

! Enable PAT overload
Router(config)# ip nat inside source list 1 interface g0/2 overload
```

4.4 ISP Router – Return Static Routes

To allow the ISP to route reply traffic back to the Sydney inside networks, static routes were added on the ISP Router pointing toward 8.8.8.1 (Sydney Router's WAN IP).

```
Router(config)# ip route 8.8.8.0 255.255.255.252 8.8.8.1
Router(config)# ip route 0.0.0.0 0.0.0.0 8.8.8.1
```

5. Verification & Test Results

5.1 Ping Test – Sydney Router to ISP Loopback

```
Router# ping 9.9.9.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 9.9.9.9, timeout is 2 seconds:
.!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

Result: PASS. The initial packet drop (.) is due to ARP table population. Subsequent packets succeeded, confirming default route and WAN link are operational.

5.2 Ping Test – ISP Router to Sydney WAN IP

```
Router# ping 8.8.8.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Result: PASS. 100% success rate confirms bidirectional reachability between ISP and Sydney Router WAN interface.

5.3 NAT Translation Table Verification

After initiating traffic from an internal host (Sydney PC1, 192.168.10.2) to the ISP loopback, the NAT translation table on Sydney Router confirmed correct PAT operation:

```
Router# show ip nat translations

Pro  Inside global    Inside local       Outside local      Outside global
icmp 8.8.8.1:61      192.168.10.2:61    9.9.9.9:61         9.9.9.9:61
icmp 8.8.8.1:62      192.168.10.2:62    9.9.9.9:62         9.9.9.9:62
icmp 8.8.8.1:63      192.168.10.2:63    9.9.9.9:63         9.9.9.9:63
icmp 8.8.8.1:64      192.168.10.2:64    9.9.9.9:64         9.9.9.9:64
```

Result: PASS. Internal host 192.168.10.2 is correctly translated to public IP 8.8.8.1 with unique port numbers, confirming PAT/overload is functioning as expected.

5.4 Summary of Tests

Test	Source	Destination	Result
Sydney Router → ISP Loopback	Router Sydney	9.9.9.9	PASS (80%)
ISP Router → Sydney WAN	ISP Router	8.8.8.1	PASS (100%)
NAT Translation – PC1 → ISP	192.168.10.2	9.9.9.9	PASS
Default route propagation via OSPF	Router Sydney	All sites	PASS

6. Issues Encountered

The following minor issues were encountered and resolved during the configuration:

Issue	Cause	Resolution
'en conf t' rejected by CLI	Cannot chain 'en' and 'conf t' in one line	Issued 'en' and 'conf t' as separate commands
'show ip nat translaitions' error	Typo in command ('translaitions')	Re-entered as 'show ip nat translations'
'access-list permit' missing list number	Missing ACL number in one entry	Re-entered with correct syntax: 'access-list 1 permit ...'
First ping packet dropped (.!!!!)	ARP table not yet populated	Expected behaviour; no action required

7. Conclusion

The ISP integration was completed successfully. The Sydney Router now acts as the network edge device, performing NAT/PAT to allow all internal subnets (Sydney LAN 1, Sydney LAN 2, Melbourne LAN 1, Melbourne LAN 2, and the inter-site WAN link) to access the simulated internet via the ISP Router.

The configuration demonstrates a real-world scenario common in small-to-medium enterprise networks where a single public IP address is shared among multiple internal hosts using PAT overload. OSPF was leveraged to redistribute the default route across the internal routing domain, ensuring Melbourne hosts can also reach the internet without manual static routes on the Melbourne Router.

All verification tests passed. The network is ready for further configuration such as access control lists, quality of service, or additional WAN redundancy.

8. Recommendations

- Add OSPF authentication on all inter-router links to prevent unauthorized route injection
- Implement inbound access-list on Gig0/2 (WAN interface) to filter unsolicited traffic from the ISP
- Configure HSRP or VRRP on Sydney Switch uplinks for gateway redundancy
- Enable 'ip nat translation timeout' tuning to reclaim NAT table entries faster in high-traffic environments
- Consider a secondary ISP connection on Router Melbourne for WAN failover
- Document the full IP scheme in a network management tool (e.g. SolarWinds, NetBox) for ongoing visibility