SOP-NET-009_MikroTik_New_Site_Deployment_v1.0

Standard Operating Procedure: MikroTik New Site Deployment

Document ID:	SOP-NET-009
Title:	MikroTik New Site Deployment
Category:	Network Infrastructure
Version:	1.0
Status:	Draft
Author:	OberaConnect
Creation Date:	2026-01-12
Approval Date:	Pending

1.0 Purpose

This procedure documents the complete workflow for deploying a new customer site with a MikroTik router and UniFi access points. It covers subnet allocation, configuration generation, router setup, and AP adoption using OberaConnect's network-config-builder tooling.

2.0 Scope

This SOP applies to: - New customer site deployments with MikroTik routers - OberaConnect technicians performing network installations - Sites using the 10.54.x.x subnet allocation scheme - Deployments with UniFi access points managed via UniFi Site Manager

3.0 Definitions

Term	Definition
RouterOS	MikroTik's proprietary operating system
Winbox	MikroTik's GUI management application
router.rsc	RouterOS script file for importing configuration
Inform URL	UniFi controller adoption URL for APs
DHCP	Dynamic Host Configuration Protocol
NAT	Network Address Translation
Bridge	Layer 2 network bridge combining multiple interfaces

4.0 Roles & Responsibilities

Role	Responsibility
Network Technician	Execute deployment, configure equipment
Project Manager	Coordinate with customer, schedule installation

Role	Responsibility
NOC	Monitor site health post-deployment

5.0 Prerequisites

5.1 Information Required

- ☐ Customer name and site location
- ☐ ISP circuit details (WAN IP, gateway, DNS servers)
- ☐ Circuit ID from ISP
- ☐ MikroTik router model (determines LAN port configuration)
- ☐ UniFi AP model(s) to be deployed

5.2 Equipment Required

- ☐ MikroTik router (factory reset or new)
- ☐ UniFi access point(s)
- ☐ Ethernet cables
- ☐ Laptop with Winbox installed
- ☐ Console cable (optional backup)

5.3 Access Required

- ☐ Physical access to site or bench setup
- ☐ UniFi Site Manager account (unifi.ui.com)
- ☐ network-config-builder tooling access

6.0 Procedure

Phase 1: Subnet Allocation

6.1 Check Available Subnet Block

```
cd /home/mavrick/Projects/network-config-builder
python3 subnet_allocator.py summary
```

Review output to see next available block in the 10.54.x.x/16 range.

6.2 Allocate Customer Subnet

```
python3 subnet_allocator.py allocate \
  --customer-id "<CIRCUIT_ID>" \
  --customer-name "<CUSTOMER_NAME>" \
  --wan-ip "<WAN_IP>/<CIDR>" \
  --wan-gateway "<GATEWAY_IP>" \
  --location "<CITY>, <STATE>" \
  --circuit-id "<FULL_CIRCUIT_ID>"
```

Example:

```
python3 subnet_allocator.py allocate \
  --customer-id "205923" \
  --customer-name "DC Lawn Foley" \
  --wan-ip "142.190.216.114/30" \
  --wan-gateway "142.190.216.113" \
```

```
  --location "Foley, AL" \
  --circuit-id "/INT/205923//UIF/"
```

This allocates 4 consecutive /24 blocks (only first is configured initially).

Phase 2: Configuration Generation

6.3 Create Customer Directory

```
mkdir -p customers/<CUSTOMER_FOLDER>/configs
```

6.4 Create customer_config.yaml

Create `customers/<CUSTOMER_FOLDER>/customer_config.yaml`:

```yaml
customer:
  name: "<CUSTOMER_NAME>"
  site: "<SITE_NAME>"
  circuit_id: "<CIRCUIT_ID>"

wan:
  type: static
  interface: ether1
  address: "<WAN_IP>/<CIDR>"
  gateway: "<GATEWAY_IP>"
  dns_servers:
    - "<PRIMARY_DNS>"
    - "<SECONDARY_DNS>"

lan:
  interface: bridge-lan
  address: "10.54.X.1/24"
  dhcp:
    pool_start: "10.54.X.100"
    pool_end: "10.54.X.200"
    lease_time: "24h"

security:
  admin_password: "<SECURE_PASSWORD>"

mikrotik:
  lan_ports: [ether2, ether3, ether4, ether5, ether6, ether7, ether8, ether9, ether10]
  timezone: America/Chicago
  enable_wan_winbox: true
  enable_wan_ssh: false
  enable_mac_discovery_lan: true
  bandwidth_test: false

unifi:
  site_id: "<UNIFI_SITE_ID>"
  inform_url: "http://<SITE_ID>.unifi-hosting.ui.com:8080/inform"
```

6.5 Generate Router Configuration

```
./network-config generate \
  -i customers/<CUSTOMER_FOLDER>/customer_config.yaml \
```

```
-o customers/<CUSTOMER_FOLDER>/configs \
-v
```

This generates `router.rsc` with all required sections.

Phase 3: Router Preparation

6.6 Factory Reset Router (If Previously Used)

1. Power off the router
2. Hold reset button while powering on
3. Continue holding for ~5 seconds until LEDs flash
4. Release - router will boot to factory defaults

6.7 Initial Connection **Option A: Winbox via Neighbors (default config only)** 1. Connect laptop to any LAN port (ether2-10) 2. Open Winbox 3. Click "Neighbors" tab 4. Select router by MAC address 5. Login: `admin` / (check device label for default password or blank)

Option B: Direct IP (after default config) 1. Connect laptop to any LAN port 2. Get DHCP address (192.168.88.x range) 3. Winbox to `192.168.88.1` 4. Login: `admin` / (device label password)

6.8 Remove Default Configuration When prompted "Do you want to remove default config?": - Select **YES** to remove default bridge configuration - This is **CRITICAL** - default config bridges ALL ports including WAN

Phase 4: Router Configuration

6.9 Remove ether1 from Bridge (If Default Config Persists) If ether1 is still bridged after factory reset:

```
/interface bridge port remove [find interface=ether1]
/ip dhcp-client remove [find]
```

Verify:

```
/interface bridge port print
```

ether1 should NOT appear in list.

6.10 Import Configuration **Method A: Full .rsc Import** 1. Upload `router.rsc` to router (Files in Winbox, drag and drop) 2. Execute:

```
/import file-name=router.rsc
```

Method B: Terminal Paste (Sectioned)

Paste configuration in sections for better troubleshooting:

Section 1: System Identity

```
/system identity set name="<CUSTOMER_NAME>"
/system clock set time-zone-name=America/Chicago
```

Section 2: WAN Configuration

```
/ip address add address=<WAN_IP>/<CIDR> interface=ether1 comment="WAN"
/ip route add gateway=<GATEWAY_IP> comment="Default Gateway"
```

Section 3: LAN Bridge

```
/interface bridge add name=bridge-lan comment="LAN Bridge"
:do { /interface bridge port add bridge=bridge-lan interface=ether2 } on-error={}
:do { /interface bridge port add bridge=bridge-lan interface=ether3 } on-error={}
:do { /interface bridge port add bridge=bridge-lan interface=ether4 } on-error={}
:do { /interface bridge port add bridge=bridge-lan interface=ether5 } on-error={}
/ip address add address=10.54.X.1/24 interface=bridge-lan comment="LAN Gateway"
```

Section 4: DNS

```
/ip dns set servers=<DNS1>,<DNS2> allow-remote-requests=yes
```

Section 5: DHCP Server

```
/ip pool add name=lan-pool ranges=10.54.X.100-10.54.X.200
/ip dhcp-server add name=lan-dhcp interface=bridge-lan address-pool=lan-pool lease-time=24h disabled=no
/ip dhcp-server network add address=10.54.X.0/24 gateway=10.54.X.1 dns-server=<DNS1>,<DNS2>
```

Section 6: NAT

```
/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade comment="NAT LAN to WAN"
```

Section 7: Firewall Input Chain

```
/ip firewall filter add chain=input connection-state=established,related action=accept
/ip firewall filter add chain=input connection-state=invalid action=drop
/ip firewall filter add chain=input in-interface=bridge-lan action=accept
/ip firewall filter add chain=input in-interface=ether1 protocol=icmp action=accept
/ip firewall filter add chain=input in-interface=ether1 protocol=tcp dst-port=8291 action=accept commen
/ip firewall filter add chain=input in-interface=ether1 action=drop
```

Section 8: Firewall Forward Chain

```
/ip firewall filter add chain=forward connection-state=established,related action=accept
/ip firewall filter add chain=forward connection-state=invalid action=drop
/ip firewall filter add chain=forward in-interface=bridge-lan action=accept
/ip firewall filter add chain=forward in-interface=ether1 connection-state=new action=drop
```

Section 9: Services

```
/ip service set winbox disabled=no
/ip service set ssh address=10.54.X.0/24 disabled=no
/ip service set telnet disabled=yes
/ip service set ftp disabled=yes
/ip service set www disabled=yes
/ip service set api disabled=yes
/ip service set api-ssl disabled=yes
```

Section 10: MAC Discovery (LAN Only)

```
/interface list add name=LAN
/interface list member add list=LAN interface=bridge-lan
/tool mac-server set allowed-interface-list=LAN
/tool mac-server mac-winbox set allowed-interface-list=LAN
/ip neighbor discovery-settings set discover-interface-list=LAN
/tool bandwidth-server set enabled=no
```

Section 11: Admin Password

```
:do { /user set admin password="<PASSWORD>" } on-error={ /user add name=admin password="<PASSWORD>" grou
```

Phase 5: Verification

6.11 Verify WAN Connectivity

```
/ping 8.8.8.8 count=5
/ping google.com count=5
```

6.12 Verify LAN Configuration

```
/ip address print
/interface bridge port print
/ip dhcp-server print
/ip pool print
```

6.13 Test Remote Access From external network: - Winbox to `<WAN_IP>:8291` - Should connect successfully

6.14 Create Backup

```
/system backup save name=<CUSTOMER>-initial-config
/export file=<CUSTOMER>-initial-config
```

Download both files via Winbox Files menu.

Phase 6: UniFi AP Adoption

6.15 Create Site in UniFi Site Manager

1. Login to unifi.ui.com
2. Click "Add Site"
3. Enter site name matching customer
4. Copy the Site ID from URL

6.16 Adopt Access Point

1. Connect AP to LAN port on MikroTik
2. Wait for AP to get DHCP address
3. SSH to AP:

```
ssh ubnt@<AP_IP>
# Default password: ubnt
```

4. Set inform URL:

```
set-inform http://<SITE_ID>.unifi-hosting.ui.com:8080/inform
```

5. In UniFi Site Manager:
   - Device appears in "Pending Adoption"
   - Click "Adopt"
   - Wait for provisioning to complete

6.17 Configure WiFi

1. In UniFi Site Manager
2. Go to Settings > WiFi
3. Create network(s) as required
4. Apply to site

7.0 Verification & Quality Checks

7.1 Deployment Checklist

- ☐ Router identity set correctly
- ☐ WAN IP responds to ping from internet
- ☐ LAN clients get DHCP addresses in correct range
- ☐ NAT working (LAN clients can browse internet)
- ☐ Winbox accessible from WAN IP
- ☐ SSH restricted to LAN only
- ☐ Firewall rules in place (6 input, 4 forward)
- ☐ Router backup saved and downloaded
- ☐ UniFi AP adopted and online
- ☐ WiFi broadcasting and clients can connect
- ☐ Site added to monitoring

8.0 Troubleshooting

Issue	Resolution
Winbox can't find router in neighbors	MAC discovery disabled by security config. Connect via direct IP instead.
"Username or password wrong" after import	Password command may have failed. Try default label password, or factory reset if needed.
WAN not working after config	Check if ether1 is still bridged: `/interface bridge port print`. Remove if present.
DHCP not assigning addresses	Verify pool exists: `/ip pool print`. Check server is enabled: `/ip dhcp-server print`.
Can't ping internet from LAN	Check NAT rule exists: `/ip firewall nat print`. Verify masquerade on srcnat chain.
AP not appearing for adoption	Verify AP has IP in LAN range. SSH to AP and run `set-inform` command manually.
Locked out after config import	Router restricts access to configured IP ranges. Connect from LAN to regain access.

9.0 Related Documents

Document	Description
SOP-NET-002	MikroTik Configuration (general)
SOP-NET-005	Ubiquiti Equipment Configuration
SOP-NET-008	UniFi Bulk Deployment
SUBNET_ALLOCATION_SCHEME.md	Customer subnet allocation documentation

---

10.0 Revision History

Version	Date	Author	Change Description
1.0	2026-01-12	OberaConnect	Initial document creation

11.0 Approval

Name	Role	Signature	Date
	Technical Lead Operations Manager		

Appendix A: MikroTik Model LAN Port Reference

Model	LAN Ports
RB4011iGS+RM	ether2-ether10, sfp-sfpplus1
hEX S (RB760iGS)	ether2-ether5
hAP ac2	ether2-ether5
CCR1009	ether2-ether8

Appendix B: Common MikroTik Default Passwords

Scenario	Username	Password
Factory new (older models)	admin	(blank)
Factory new (newer models)	admin	Device label password
After “Remove Config”	admin	(blank)

Appendix C: Quick Reference Commands

```
# Check current config
/export

# View interfaces
/interface print

# View IP addresses
/ip address print

# View firewall rules
/ip firewall filter print
/ip firewall nat print

# View DHCP leases
/ip dhcp-server lease print

# Backup configuration
/system backup save name=backup
/export file=backup

# Factory reset
/system reset-configuration no-defaults=yes
```