

=====

=====

## CATEGORY: Network

=====

=====

Network operations directly affect connectivity, diagnostics, and service availability. These SOPs ensure every network action performed through RDAM Script Wizard is controlled, auditable, and aligned with enterprise operational and security standards.

## SOP 1 – Get Local IP Configuration

**Script Name:** Get Local IP Configuration **Category:** Network **Version:** 1.0 **Approved By:** IT Operations / Security

### 1. Purpose

This script retrieves detailed IP configuration information from the local system, supporting troubleshooting, inventory, and network diagnostics.

### 2. Scope

- **Systems:** Windows servers and workstations
- **Interfaces:** Physical NICs, virtual NICs, wireless adapters, VPN adapters
- **Authorized Personnel:**
  - System administrators
  - Network engineers
  - Helpdesk Tier-2/3

### 3. Definitions

- **IP Configuration:** Includes IP address, subnet mask, gateway, DNS servers.
- **Interface:** Network adapter on the system.

### 4. Preconditions

- Operator must have permission to query system network configuration.

- System must be reachable.
- Network stack must be operational.

## 5. Required Inputs

- None (full enumeration)
- Optional: Specific interface name filter

## 6. Procedure Steps

### 1. Input Collection

- Wizard prompts for optional interface filter.

### 2. Interface Enumeration

- Retrieve all network interfaces.
- Apply filter if provided.

### 3. Configuration Retrieval

- For each interface, retrieve:
  - IPv4/IPv6 addresses
  - Subnet mask/prefix length
  - Default gateway
  - DNS servers
  - DHCP status
  - MAC address
  - Link status

### 4. Output Formatting

- Present structured results grouped by interface.

### 5. Logging

- Log operator, filters, timestamp.

## 7. Expected Output

- Full IP configuration for all or filtered interfaces.

## 8. Post-Execution Validation

- Operator may verify using `ipconfig` or `Get-NetIPConfiguration`.

## 9. Error Handling

- No interfaces found
- Invalid filter
- Access denied

## 10. Security Considerations

- IP configuration may reveal sensitive network details.
- Access should be restricted to authorized personnel.

## 11. Audit Logging Requirements

- Operator ID
- Filter used
- Timestamp

## 12. Organizational Benefit Statement

This script provides a consistent, auditable method for retrieving IP configuration, supporting troubleshooting and network diagnostics.

# SOP 2 – Test Network Connectivity (Ping)

**Script Name:** Test Network Connectivity (Ping) **Category:** Network

## 1. Purpose

This script tests basic network connectivity to a specified host using ICMP echo requests. It supports troubleshooting, availability checks, and network diagnostics.

## 2. Scope

- **Targets:** Hostnames or IP addresses
- **Use Cases:**
  - Connectivity validation
  - Troubleshooting network outages
  - Verifying DNS resolution

## 3. Definitions

- **Ping:** ICMP echo request/response test.

- **Round-Trip Time (RTT):** Time for packet to travel to target and back.

## 4. Preconditions

- Operator must have permission to run network diagnostics.
- ICMP must be allowed by local and remote firewalls.
- Target must be reachable on the network.

## 5. Required Inputs

- Target hostname or IP
- Optional: Number of attempts
- Optional: Timeout value

## 6. Procedure Steps

### 1. Input Collection

- Wizard prompts for target and optional parameters.

### 2. Input Validation

- Validate hostname/IP format.
- Validate numeric parameters.

### 3. DNS Resolution

- Resolve hostname to IP (if applicable).
- Log resolution result.

### 4. Ping Operation

- Send ICMP echo requests.
- Capture:
  - Success/failure
  - RTT
  - Packet loss

### 5. Output Formatting

- Present summary and per-attempt results.

### 6. Logging

- Log target, attempts, operator, timestamp.

## 7. Expected Output

- Connectivity status
- RTT metrics
- Packet loss percentage

## 8. Post-Execution Validation

- Operator may test with `ping` or `Test-Connection`.

## 9. Error Handling

- Host unreachable
- DNS failure
- ICMP blocked
- Invalid input

## 10. Security Considerations

- Excessive pinging may trigger IDS alerts.
- Use only for authorized diagnostics.

## 11. Audit Logging Requirements

- Operator ID
- Target
- Attempt count
- Timestamp

## 12. Organizational Benefit Statement

This script provides a standardized, auditable method for testing network connectivity, improving troubleshooting efficiency and reducing downtime.

# SOP 3 – Test Port Connectivity (TCP)

**Script Name:** Test Port Connectivity (TCP) **Category:** Network

## 1. Purpose

This script tests TCP connectivity to a specified host and port, supporting troubleshooting of application connectivity, firewall rules, and service availability.

## 2. Scope

- **Targets:** Hostnames or IPs
- **Ports:** Any TCP port
- **Use Cases:**
  - Application troubleshooting
  - Firewall validation
  - Service availability checks

## 3. Definitions

- **TCP Port Test:** Attempt to establish a TCP connection to a remote port.
- **Timeout:** Maximum time to wait for connection.

## 4. Preconditions

- Operator must have permission to run network diagnostics.
- Target host must be reachable.
- Remote service must be listening on target port.

## 5. Required Inputs

- Hostname or IP
- TCP port number
- Optional: Timeout value

## 6. Procedure Steps

### 1. Input Collection

- Wizard prompts for host, port, and timeout.

### 2. Input Validation

- Validate port is numeric and within 1–65535.
- Validate hostname/IP format.

### 3. DNS Resolution

- Resolve hostname to IP if needed.

### 4. TCP Connection Attempt

- Attempt to open TCP socket to target.

- Capture:
  - Success/failure
  - Connection time
  - Error reason (timeout, refused, unreachable)

## 5. Output Formatting

- Present structured results.

## 6. Logging

- Log host, port, operator, timestamp.

## 7. Expected Output

- Clear indication of whether the port is open, closed, or filtered.

## 8. Post-Execution Validation

- Operator may verify with `Test-NetConnection` or `telnet`.

## 9. Error Handling

- Port closed
- Host unreachable
- DNS failure
- Timeout

## 10. Security Considerations

- Port scanning behavior must be avoided; test only authorized ports.
- Results may reveal sensitive service information.

## 11. Audit Logging Requirements

- Operator ID
- Host
- Port
- Timestamp

## 12. Organizational Benefit Statement

This script provides a controlled, auditable method for testing TCP connectivity, supporting application troubleshooting and firewall validation.

