==========

==========

CATEGORY: NetworkAdvanced

==========

==========

Advanced network operations directly affect routing behavior, traffic flow, and system-level connectivity. These SOPs ensure every action performed through RDAM Script Wizard is **controlled**, **auditable**, and aligned with **enterprise networking and security standards**.

SOP 1 – Get ARP Table

Script Name: Get ARP Table **Category:** NetworkAdvanced **Version:** 1.0 **Approved By:** IT Operations / Network Engineering

1. Purpose

This script retrieves the system's Address Resolution Protocol (ARP) table, mapping IPv4 addresses to MAC addresses. It supports troubleshooting, network diagnostics, and security investigations.

2. Scope

- **Systems:** Windows servers and workstations
- **Data:** IPv4 ARP cache entries
- **Authorized Personnel:**
    - Network engineers
    - System administrators
    - Security analysts

3. Definitions

- **ARP Table:** Cache of IP → MAC mappings.
- **Dynamic Entry:** Learned automatically.
- **Static Entry:** Manually configured.

4. Preconditions

- Operator must have permission to query network configuration.
- Network stack must be operational.

5. Required Inputs

- None (full ARP table retrieval)

6. Procedure Steps

1. **Initialize Query**
    - Load networking APIs.
    - Validate system supports ARP enumeration.
2. **Retrieve ARP Table**
    - Enumerate all ARP entries.
    - Extract:
        - IP address
        - MAC address
        - Entry type (dynamic/static)
        - Interface index
3. **Filter (Optional)**
    - If script supports filtering, apply IP or interface filters.
4. **Output Formatting**
    - Present structured table of ARP entries.
5. **Logging**
    - Log operator, timestamp, and entry count.

7. Expected Output

- Full ARP table with IP/MAC mappings.

8. Post-Execution Validation

- Operator may verify using `arp -a`.

9. Error Handling

- Access denied
- Network stack unavailable
- No ARP entries found

10. Security Considerations

- ARP data may reveal internal network structure.
- Access should be restricted.

11. Audit Logging Requirements

- Operator ID
- Entry count
- Timestamp

12. Organizational Benefit Statement

This script provides a consistent, auditable method for retrieving ARP data, supporting troubleshooting and security investigations.

SOP 2 – Get Routing Table

Script Name: Get Routing Table **Category:** NetworkAdvanced

1. Purpose

This script retrieves the system’s routing table, showing how network traffic is directed. It supports troubleshooting, network design validation, and security analysis.

2. Scope

- **Systems:** Windows servers and workstations
- **Data:** IPv4 and IPv6 routes
- **Use Cases:**
    - Connectivity troubleshooting
    - Route validation
    - VPN diagnostics

3. Definitions

- **Route:** Instruction for forwarding packets.
- **Metric:** Priority of route.
- **Gateway:** Next hop address.

4. Preconditions

- Operator must have permission to query routing configuration.
- Network stack must be operational.

5. Required Inputs

- None (full routing table retrieval)

6. Procedure Steps

1. **Initialize Query**
    - Load routing APIs.
2. **Retrieve Routing Table**
    - Enumerate all routes.
    - Extract:
        - Destination prefix
        - Gateway
        - Interface index
        - Metric
        - Route type (static/dynamic)
3. **Optional Filtering**
    - Filter by interface, prefix, or route type.
4. **Output Formatting**
    - Present structured routing table.
5. **Logging**
    - Log operator, timestamp, route count.

7. Expected Output

- Full routing table with all active routes.

8. Post-Execution Validation

- Operator may verify using `route print` or `Get-NetRoute`.

9. Error Handling

- Access denied
- No routes found
- Network stack unavailable

10. Security Considerations

- Routing data reveals network topology; restrict access.

11. Audit Logging Requirements

- Operator ID
- Route count
- Timestamp

12. Organizational Benefit Statement

This script provides a controlled, auditable method for retrieving routing information, supporting troubleshooting and network design validation.

SOP 3 – Add Static Route

Script Name: Add Static Route **Category:** NetworkAdvanced

1. Purpose

This script adds a static route to the system's routing table, directing traffic for a specific network through a specified gateway. It supports advanced troubleshooting, network segmentation, and application-specific routing.

2. Scope

- **Systems:** Windows servers and workstations
- **Routes:** IPv4 and IPv6
- **Use Cases:**
    - VPN routing
    - Application-specific routing

- Network isolation

3. Definitions

- **Static Route:** Manually configured route that persists until removed.
- **Prefix:** Network address and mask.

4. Preconditions

- Operator must have administrative rights.
- Gateway must be reachable.
- Route must not conflict with existing critical routes.
- Action must be authorized.

5. Required Inputs

- Destination prefix (e.g., 10.20.30.0/24)
- Gateway IP
- Interface index or name
- Optional: Metric
- Optional: Persistent flag

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for prefix, gateway, interface, and options.
2. **Validation**
    - Validate prefix format.
    - Validate gateway IP.
    - Validate interface exists.
3. **Conflict Check**
    - Check for existing identical or overlapping routes.
    - If conflict found, abort unless override allowed.
4. **Add Route**
    - Add static route using appropriate API.
    - Apply persistence if selected.

5. **Post-Add Verification**
    - Requery routing table to confirm route exists.
6. **Logging**
    - Log prefix, gateway, interface, operator, timestamp.

7. Expected Output

- Confirmation that static route was added.

8. Post-Execution Validation

- Operator may test connectivity using `ping` or `tracert`.

9. Error Handling

- Invalid prefix
- Gateway unreachable
- Access denied
- Route conflict

10. Security Considerations

- Incorrect routes can break connectivity.
- Unauthorized routing changes can create security gaps.

11. Audit Logging Requirements

- Operator ID
- Prefix
- Gateway
- Interface
- Timestamp

12. Organizational Benefit Statement

This script ensures static routes are added safely and with full accountability, supporting advanced networking scenarios without risking misconfiguration.

SOP 4 – Remove Static Route

Script Name: Remove Static Route **Category:** NetworkAdvanced

1. Purpose

This script removes a static route from the system’s routing table. It supports cleanup, troubleshooting, and rollback of temporary routing changes.

2. Scope

- **Systems:** Windows servers and workstations
- **Routes:** IPv4 and IPv6 static routes

3. Definitions

- **Static Route Removal:** Deleting a manually configured route.

4. Preconditions

- Operator must have administrative rights.
- Route must exist.
- Removal must be authorized.

5. Required Inputs

- Destination prefix
- Optional: Gateway
- Optional: Interface

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for prefix and optional parameters.
2. **Route Resolution**
    - Identify matching static route(s).
    - If none found, return informational message.
3. **Safety Check**
    - Ensure route is not critical for system connectivity.
4. **Remove Operation**
    - Remove route using appropriate API.
5. **Post-Removal Verification**
    - Requery routing table to confirm removal.

6. **Logging**
    - Log prefix, gateway (if applicable), operator, timestamp.

7. Expected Output

- Confirmation that static route was removed.

8. Post-Execution Validation

- Operator may test connectivity to ensure no unintended impact.

9. Error Handling

- Route not found
- Access denied
- Removal breaks connectivity (must be documented)

10. Security Considerations

- Removing routes may disrupt services.
- Must follow change-control procedures.

11. Audit Logging Requirements

- Operator ID
- Prefix
- Gateway (if applicable)
- Timestamp

12. Organizational Benefit Statement

This script ensures static routes are removed safely and with full accountability, supporting cleanup and troubleshooting without risking network outages.