GENERAL

nec 80573 user guide

Published: September 3, 2026 | Index ID: #-

NEC 80573 User Guide: A Complete Reference for Installation, Configuration, and Maintenance

Welcome to the definitive NEC 80573 user guide. Whether you are a seasoned network engineer, a system administrator, or a new user who has just acquired the NEC 80573 device, this guide is designed to walk you through every step of the process – from unboxing and physical setup to advanced configuration and troubleshooting. By the end of this article, you will have a solid understanding of how to harness the full capabilities of the NEC 80573, ensuring optimal performance and reliability in your environment.

Table of Contents

1. Product Overview
2. Key Features
3. System Requirements and Compatibility
4. Unboxing and Physical Setup
5. Initial Setup and Configuration
6. Advanced Configuration Options
7. Security Best Practices
8. Troubleshooting Common Issues
9. Routine Maintenance and Updates
10. Frequently Asked Questions
11. Conclusion

1. Product Overview

The NEC 80573 is a high-performance, multi-protocol network device that integrates seamlessly into a wide range of enterprise infrastructures. Designed for reliability and scalability, the 80573 supports both IPv4 and IPv6, offers robust QoS mechanisms, and is built to withstand demanding environments.

Whether you need a secure gateway for a small office or a high-throughput router for a data center, the NEC 80573 delivers the flexibility and performance required by modern networks.

2. Key Features

- Dual-Stack Support: Full IPv4/IPv6 compatibility ensures smooth transition to next-generation IP addressing.
- High Throughput: Up to 10 Gbps line rate with low latency, suitable for bandwidth-intensive applications.
- Advanced QoS: Traffic shaping, priority queuing, and bandwidth management help maintain application performance.
- Robust Security: Integrated firewall, IPS/IDS, and support for VPN protocols (IPSec, OpenVPN, L2TP).
- Modular Design: Hot-swappable power supplies and redundant fan modules for high availability.
- Comprehensive Management: Web-based GUI, SNMP v3, CLI, and RESTful APIs for flexible administration.
- Energy Efficiency: Power-saving modes reduce operational costs.
- Extensive Logging: Syslog, RADIUS, TACACS+ support for audit trails and compliance.

3. System Requirements and Compatibility

Before you begin, ensure your environment meets the following prerequisites:

- Operating System: Windows 10/11, macOS 12+, Linux (Ubuntu 20.04+, CentOS 8+, Debian 10+).
- Network Interface: 1 Gbps Ethernet port available for management access.
- Power Supply: 220V AC, 50/60 Hz.
- Firmware: Latest NEC 80573 firmware (downloadable from NEC support portal).
- Software Tools: NEC 80573 Configuration Utility, SSH client (PuTTY, OpenSSH).
- Browser: Latest version of Chrome, Firefox, Edge, or Safari for GUI access.

4. Unboxing and Physical Setup

4.1. What's Inside the Box?

The NEC 80573 package typically includes:

- NEC 80573 chassis
- Power adapter (dual-voltage)
- Management Ethernet cable (Cat6)
- Quick Start Guide (this user guide)
- Warranty card and registration form

4.2. Mounting the Device

1. Rack Mounting: The chassis supports 1U or 2U rack mounting. Use the included mounting rails and screws. Ensure the device is level and securely fastened.
2. Ventilation: Position the 80573 in a well-ventilated area. Avoid placing it near heat sources or in enclosed spaces.
3. Power Connection: Connect the power adapter to the device and then to a grounded outlet. Verify the power indicator lights up.

4.3. Initial Power-On

Once the device is powered, the LED status panel will indicate:

- Power LED: Solid green indicates normal operation.
- System LED: Flashing during boot; solid green when ready.
- Interface LEDs: Each Ethernet port will show link/activity status.

Wait until the system LED stabilizes before proceeding to the software setup.

5. Initial Setup and Configuration

5.1. Accessing the Web-Based GUI

By default, the NEC 80573 assigns the management IP address 192.168.1.1. Connect your computer to the management port using the provided Ethernet cable. Configure your PC with a static IP in the same subnet (e.g., 192.168.1.10) and open a web browser to http://192.168.1.1.

Login credentials:

- Username: admin
- Password: admin123

Upon first login, you will be prompted to change the password. Choose a strong password following your

organization’s policy.

5.2. Running the Initial Wizard

The web interface offers a setup wizard that guides you through the essential configuration steps:

1. Network Settings: Assign a static IP, subnet mask, gateway, and DNS servers for the management interface.
2. Time Configuration: Set the correct time zone and enable NTP for accurate logging.
3. Device Naming: Assign a meaningful hostname and location tag for easy identification.
4. Admin Account: Create or modify administrator accounts and set role-based access controls.
5. Initial Firmware Check: Verify that the firmware version matches the latest release.

5.3. Verifying Connectivity

After the wizard completes, confirm connectivity by pinging the device from your host:

```
ping 192.168.1.1
```

Also, verify that you can access the SSH interface (default port 22). Use an SSH client to connect:

```
ssh admin@192.168.1.1
```

Enter the new password when prompted.

6. Advanced Configuration Options

6.1. VLAN and Trunking

The NEC 80573 supports IEEE 802.1Q VLAN tagging. To configure VLANs:

1. Navigate to Network > VLAN in the GUI.
2. Click Add VLAN and assign a VLAN ID (e.g., 10).
3. Set the VLAN name and optional description.
4. Under Interface Settings, select the ports that will carry the VLAN (access or trunk).
5. For trunk ports, enable Allowed VLANs and specify the VLAN IDs.

6.2. QoS Policies

Quality of Service (QoS) helps prioritize critical traffic. Configure QoS as follows:

1. Go to Traffic Management > QoS.
2. Create a new Traffic Class (e.g., Voice, Video, Data).
3. Assign priority levels (High, Medium, Low) and bandwidth limits.
4. Map traffic types to classes using Policy Rules (e.g., match port, IP protocol, or DSCP value).
5. Apply the policy to the desired interfaces.

6.3. VPN Configuration

NEC 80573 supports multiple VPN types. Here’s how to set up an IPSec site-to-site VPN:

1. Navigate to VPN > IPSec.
2. Click Add Tunnel and provide a name.
3. Enter Remote Gateway IP and Local/Remote Subnets.
4. Configure the Security Association parameters: encryption algorithm (AES-256), authentication method (SHA-256), and pre-shared key.
5. Enable Auto-Start and Keep-Alive options.

6. Save and apply changes.

6.4. Firewall and Access Control Lists (ACLs)

To create a firewall rule:

1. Open Security > Firewall.
2. Select ACLs and click Add ACL.
3. Define the rule type (Allow/Deny), source/destination IPs, ports, and protocols.
4. Assign the ACL to an interface or a specific VLAN.
5. Enable logging for critical rules.
6. Apply the ACL to the interface.

6.5. SNMP Configuration

SNMP v3 provides secure monitoring. Configure as follows:

1. Navigate to Management > SNMP.
2. Enable SNMP v3 and create a user with authentication (MD5/SHA) and privacy (DES/AES) protocols.
3. Set the Community String for SNMP v2c if required.
4. Configure Trap Destinations for alert notifications.
5. Save and restart the SNMP service.

6.6. Logging and Syslog

Configure syslog to forward logs to a central server:

1. Go to System > Logging.
2. Enable Syslog and specify the server IP, port (default 514), and protocol (UDP/TCP).
3. Set the logging level (Error, Warning, Info, Debug).
4. Define log rotation policies and retention periods.
5. Apply changes and verify logs are received on the server.

7. Security Best Practices

- Change Default Credentials: Immediately replace admin passwords and disable unused accounts.
- Enable Two-Factor Authentication (2FA): If supported, integrate with your organization’s MFA solution.
- Apply Least Privilege: Grant users only the permissions necessary for their role.
- Regular Firmware Updates: Keep the device at the latest stable firmware to mitigate vulnerabilities.
- Network Segmentation: Place critical devices on separate VLANs or subnets.

Tags: #80573 #user #guide