DNP3 Protocol

Distributed Network Protocol for Critical Infrastructure

OT Security Learning Series

Document 202 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

DNP3 (Distributed Network Protocol 3) is a set of communication protocols used primarily in utilities such as electric, water, and gas systems. Developed in the 1990s by Westronic (now GE Grid Solutions), it was designed to provide reliable communication between control centers and remote substations.

Information

DNP3 is the dominant SCADA protocol in North American utilities and is widely used in electric power, water/wastewater, and oil/gas industries. Understanding DNP3 is essential for securing critical infrastructure.

1.1 Why DNP3 Matters

- **Critical infrastructure:** Powers electric grids, water systems, pipelines
- **Reliability focus:** Designed for noisy, unreliable communication links
- **Feature-rich:** Supports time synchronization, file transfer, secure authentication
- **Attack target:** Used in nation-state attacks (Ukraine 2015/2016)

2 Protocol Overview

2.1 Protocol Stack

DNP3 uses a layered architecture based on the EPA (Enhanced Performance Architecture) model:

Layer	Function
Application Layer	Data objects, function codes, fragments
Transport Layer	Segmentation and reassembly of messages
Data Link Layer	Framing, addressing, error detection (CRC)
Physical Layer	Serial (RS-232/485) or TCP/IP (port 20000)

2.2 Communication Model

DNP3 Architecture

- **Master:** Control center, SCADA system (initiates requests)
- **Outstation:** RTU, IED, or data concentrator (responds to requests)
- **Addresses:** 16-bit source and destination addresses (0–65519)
- **Unsolicited responses:** Outstations can send data without polling

2.3 Data Objects

DNP3 organizes data into object groups and variations:

Group	Type	Description
1, 10	Binary Input/Output	Digital status points and controls
20, 21	Counters	Accumulated values, pulses
30, 40	Analog Input/Output	Measurements and setpoints
50	Time and Date	Time synchronization objects
70	File Transfer	File read/write operations

3 Function Codes

DNP3 defines numerous function codes for different operations:

Code	Function	Description
0x00	Confirm	Acknowledge receipt of data
0x01	Read	Request data from outstation
0x02	Write	Send data to outstation
0x03	Select	Select control point (SBO)
0x04	Operate	Execute selected control (SBO)
0x05	Direct Operate	Immediate control execution
0x0D	Cold Restart	Restart device completely
0x0E	Warm Restart	Restart application layer
0x81	Response	Standard response from outstation
0x82	Unsolicited Response	Event-driven data from outstation

Warning

Function codes 0x02 (Write), 0x05 (Direct Operate), 0x0D, and 0x0E (Restart) can cause immediate physical impact. Without authentication, attackers can manipulate grid equipment.

4 Security Concerns

4.1 Original Protocol Weaknesses

Critical

Legacy DNP3 lacks security:

- No authentication in original specification
- No encryption – all data transmitted in cleartext
- Predictable sequence numbers enable replay attacks
- Broadcast addresses allow mass device manipulation

4.2 Real-World Attacks

DNP3 was exploited in the 2015 and 2016 Ukraine power grid attacks:

- Attackers sent unauthorized control commands via DNP3
- Direct Operate commands opened circuit breakers

- Firmware was corrupted to disable protective relays
- Over 230,000 customers lost power

4.3 Common Attack Vectors

1. **Reconnaissance:** Scanning for DNP3 devices (port 20000)
2. **Traffic analysis:** Capturing operational data and control sequences
3. **Replay attacks:** Recording and replaying valid control commands
4. **Command injection:** Sending unauthorized Direct Operate commands
5. **Firmware attacks:** Exploiting file transfer for malicious uploads

5 DNP3 Secure Authentication

IEEE 1815 introduced Secure Authentication (SA) to address DNP3 security gaps.

5.1 Security Mechanisms

Key Point

DNP3-SA provides:
- Challenge-response authentication using HMAC
- Protection against replay attacks
- Aggressive mode for reduced latency
- Key change procedures for credential management

5.2 SA Versions

Version	Features
SAv2	Basic HMAC authentication, manual key management
SAv5	Improved key management, asymmetric key support, IEC 62351-5 alignment
SAv6	Enhanced security, TLS support, certificate-based authentication

Tip

SAv5 is the current recommended version. It supports both symmetric (pre-shared keys) and asymmetric (certificate-based) authentication methods.

6 Security Mitigations

6.1 Protocol-Level Security

- **Enable Secure Authentication:** Deploy SAv5 on all DNP3 communications

- **Use TLS:** Encrypt DNP3/TCP with TLS 1.2 or higher
- **Implement key management:** Rotate authentication keys regularly
- **Disable unnecessary functions:** Block file transfer if not required

6.2 Network-Level Controls

- **Network segmentation:** Isolate DNP3 traffic in dedicated networks
- **Firewalls:** Restrict port 20000 to authorized masters only
- **IDS/IPS:** Deploy DNP3-aware intrusion detection
- **VPN tunnels:** Encrypt WAN communications

7 Further Reading

Standards and Specifications

- **IEEE 1815-2012** – DNP3 Standard
  https://standards.ieee.org/standard/1815-2012.html
- **DNP Users Group** – Technical Resources
  https://www.dnp.org/

Security Resources

- **CISA** – ICS-CERT DNP3 Advisories
  https://www.cisa.gov/news-events/ics-advisories
- **NIST SP 800-82 Rev. 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Books

- Gordon Clarke – *Practical Modern SCADA Protocols* (Newnes)