

OT PROTOCOL PRIMERS

DNP3

BACKGROUND

DNP3, “Distributed Network Protocol” is a data communication protocol originally developed by Harris, Distributed Automation Products. DNP3 enables interoperability for utility equipment via a communication standard. In 1993, ownership of the protocol was transferred to the DNP3 Users Group (a consortium of utilities and vendors). Now, the standard is maintained by IEEE Std 1815 and be accessed at: <https://standards.ieee.org>

The protocol is primarily used in the electric utility industry, but can also be found in water/waste water, transport, and oil/gas industries. [2]

FUNDAMENTALS

- DNP3 uses a client/master-> server/outstation model. [1]
- DNP3 supports transport over different network types: Point-to-Point (RS-232, RS-485), TCP/IP. [1]
- DNP3 over IP uses port **20000** by default. [3]
- DNP3 supports encrypted communication via TLS on port 19999. [3]
- DNP3 leverages an object-oriented model for describing process controls and devices. [1]

COMMUNICATION

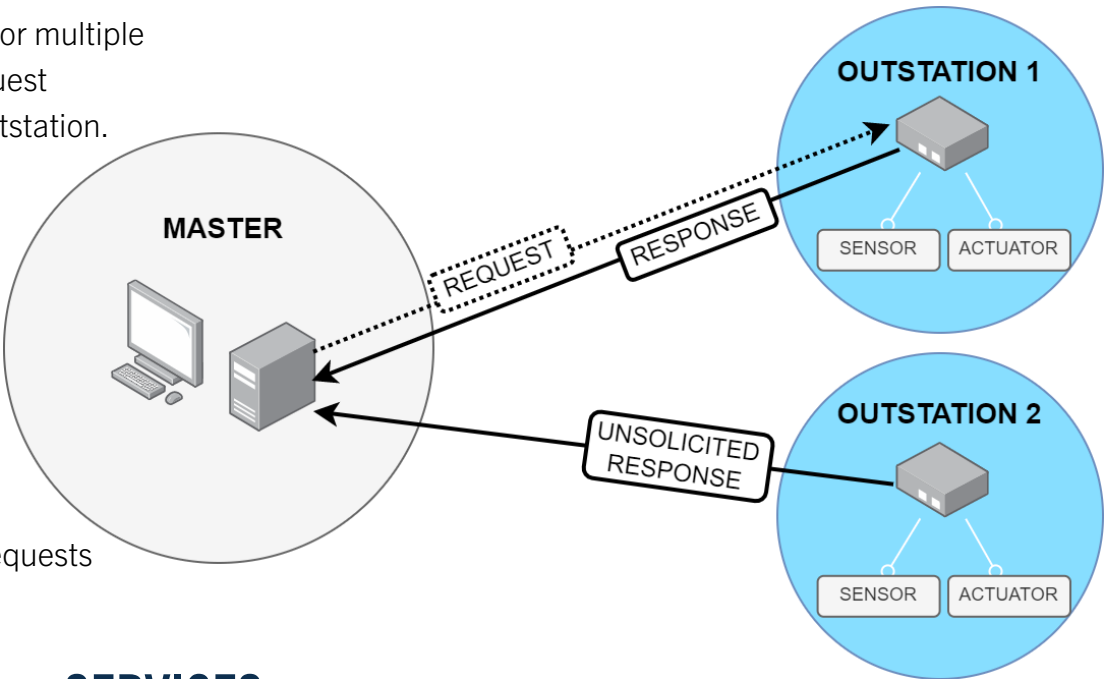
Typical DNP3 communication has a Master polling one or multiple Outstations. A **poll** starts with the Master sending a request message and follows with a response from the target outstation.

If an Outstation needs to communicate outside a poll, it can be configured to send an **unsolicited response**.

DNP3 exposes data as standardized **objects** which are classified by a **group** and **variation** pair.

A master can request multiple objects by specifying a **class**. Transported data can range from point values, events, files, and more.

A commonly used message is an **integrity poll**, which requests class 0,1,2, & 3 data from an outstation. [1]



SERVICES

DNP3 defines several services to allow for remote monitoring and control of outstations.

Category	Service	Description	Code	Hex
DATA ACCESS	Read	Read one or more data objects from a device.	1	0x01
	Write	Write one or more data objects on a device.	2	0x02
SIGNAL CONTROL	Select , Operate	A two-part command sequence to manipulate an output (select then operate).	3 4	0x03 0x04
	Direct Operate	A single command to manipulate an output.	5	0x05
DEVICE MANAGEMENT	Cold Restart ,	Force the outstation to restart.	14	0x0D
	Enable Unsolicited Responses , Disable Unsolicited Responses	Configure the outstation’s ability to send unsolicited responses.	20 21	0x14 0x15

[4]

DATA STRUCTURES

ALL GROUPS	Group	Description	Group	Description	TOP OBJECTS	Name	Grp	Var	Description
	0	Device Attributes	60-69	Class		Device Info	0	250	Device name and model
	1-9	Binary Inputs	70-79	Files		Class Objects	60	1,2,3,4	Poll a group of objects (0,1,2,3)
	10-19	Binary Outputs	80-82	Devices		Binary Output	12	1	Control a binary output
	20-29	Counters	83-89	Data Sets		Analog Output	41	1	Control an analog output
	30-39	Analog Inputs	90-99	Applications		Time and Date	50	1	Get or set outstation time
	40-49	Analog Outputs	100-119	Alt Num / Other		File Transport	70	5	Read or write file data
	50-59	Time	120-129	Security		Authentication	120	1,2	Challenge and response

[4]

[4]

REFERENCES

[1] Curtis, K. (2005). *A DNP3 Protocol Primer*. DNP Users Group.
<https://www.dnp.org/Portals/0/AboutUs/DNP3%20Primer%20Rev%20A.pdf>

[2] DNP.ORG (2024). *Overview of DNP3 Protocol*.
<https://www.dnp.org/About/Overview-of-DNP3-Protocol>

[3] Internet Assigned Numbers Authority. (2024). *Service Name and Transport Protocol Port Number Registry*.
<https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt>

[4] Bloice, G., Bontje, C. (2023). *packet-dnp.c*. Wireshark.
<https://github.com/wireshark/wireshark/blob/master/epan/dissectors/packet-bacapp.c>