DNP3

S.Venkatesan

Acknowledgement: The contents, example scripts and some figures are copied from various sources.
Thanks to all authors and sources made those contents public and usable for educational purpose

Distributed Network Protocol 3 (DNP3)

- Its main use is in utilities such as electric and water companies.

- **DNP3 uses a Master/Remote Model:** DNP3 is typically used between centrally located masters and distributed remotes.

- The master provides the interface between the human network manager and the monitoring system.

- The remote (RTUs and intelligent electronic devices) provides the interface between the master and the physical device(s) being monitored and/or controlled.

- The DNP3 protocol is a polled protocol.
  - When the master station connects to a remote, an integrity poll is performed.
  - Integrity polls are important for DNP3 addressing. This is because they return all buffered values for a data point and include the current value of the point as well.

- The DNP3 protocol is compliant with IEC 62351-5.

Main DNP3 Capabilities

- As an intelligent and robust SCADA protocol, DNP3 gives many capabilities. Some of them are:
  - DNP3 can request and respond with multiple data types in single messages
  - Response without request (unsolicited messages)
  - It allows multiple masters and peer-to-peer operations
  - It supports time synchronization and a standard time format
  - It includes only changed data in response messages.

Features

- It makes heavy use of cyclic redundancy check codes to detect errors.

- The improved bandwidth efficiency is accomplished through event oriented data reporting.
  - These events are each placed in one of three buffers, associated with "Classes" 1, 2 and 3. In addition to these, Class 0 is defined as the "static" or current status of the monitored data.

Function Codes

- DNP3 uses 27 basic function codes to exchange information between Masters (for example Control Center) and Remotes (for example pump yard).
  - Some of those function codes enable a Master to request and receive status information from a Remote.
  - Other function codes enable a Master to determine or adjust the configuration of a Remote.

- Several function codes are defined for a DNP3 Master to control the Remote itself or equipment co-located with the Remote.

- One function code is provided to enable the Remote to respond autonomously with an Unsolicited Message to particular events that occur in its installation space.

- Example
  - Master to request and receive status info from a Remote
  - Master to change a Remote's settings
  - Master to control the Remote
  - Remote to send an unsolicited response about particular events that occur in its area

DNP3 Unsolicited Response Limitations

- Key limitation of all unsolicited ("asynchronous") alerts: there's no "keep alive" function.

- For polled ("synchronous") protocols, the manager polls the agent. This guarantees that a disabled agent will be promptly identified at the next polling cycle.

- Contrast this with what happens in an unsolicited-message protocol: a disabled agent remains silent.
  - This silence is identical to an active agent reporting that "I have no problems right now."

- That's why, whenever possible, you should look for a DNP3 master that has some ability to routinely query agents for their status.
  - This mitigates one of the major threats from using DNP3.

What are the challenges of using unsolicited responses?

- Data loss can occur if the device has a limited buffer size and a timeout period for storing unsolicited data, after which it will discard them.

- Data duplication can also occur, as the same data may be sent both unsolicitedly and in response to a poll.

- Data synchronization can also be affected, as the master may not have a complete and consistent view of the device state.

- To address these issues,
  - the master should use timestamps, sequence numbers, and integrity polls to verify and update the data,
  - while the device should mark data as sent after sending an unsolicited response and clear the mark after receiving a confirmation from the master.

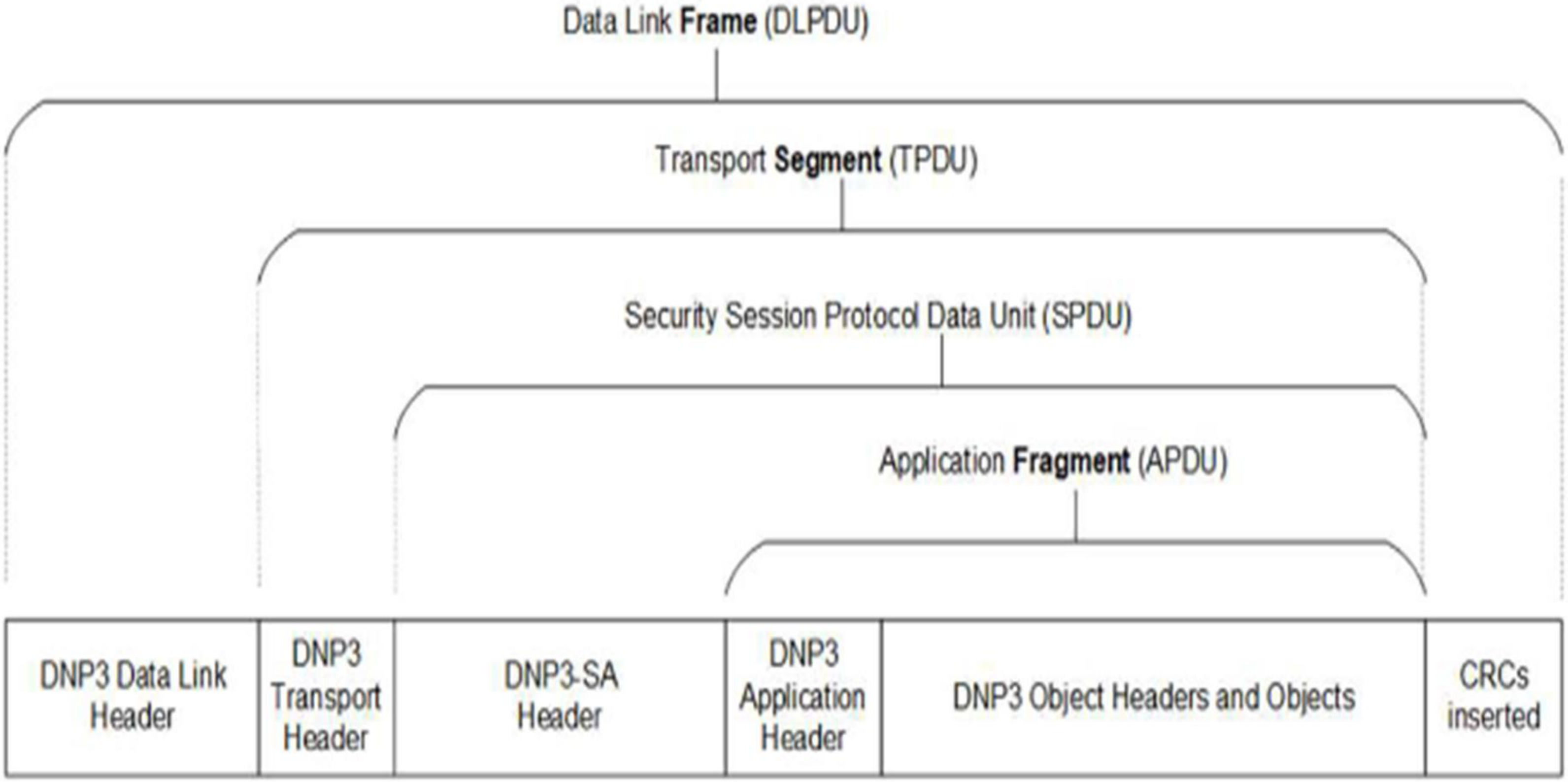
Intelligent Electronic Devices

- In the electric power industry, an **intelligent electronic device** (**IED**) is an integrated microprocessor-based controller of power system equipment, such as circuit breakers, transformers and capacitor banks.

- Similar to a PLC, an intelligent end device (IED) can establish communication between remote sensors and controllers and the communications network.

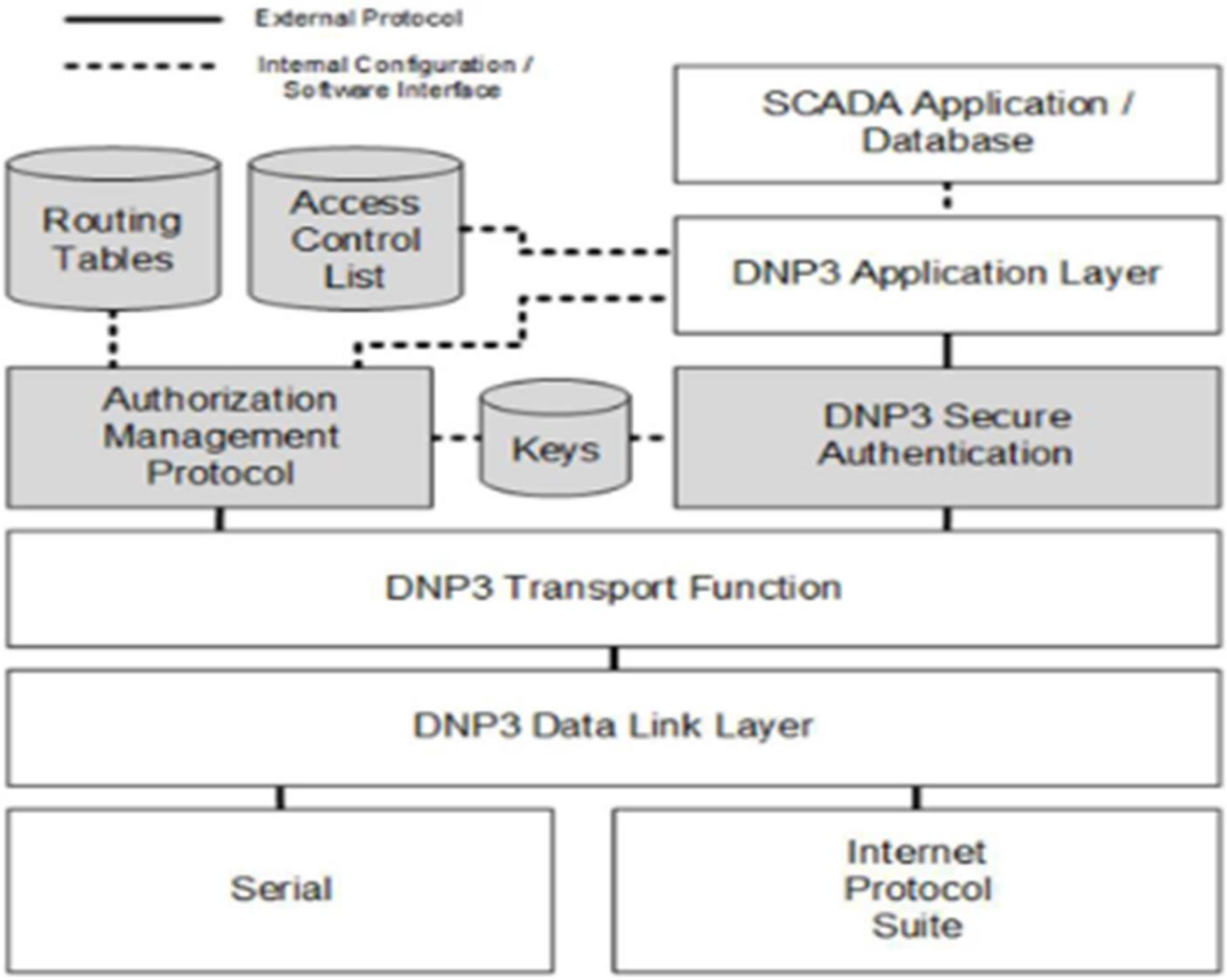
- An IED differs from a PLC in that a single IED can control several different aspects of a piece of equipment, so that the entire piece of equipment works in harmony with the rest of the needs of the system and within established design parameters.

DNP3 Secure Authentication (DNP3-SA)

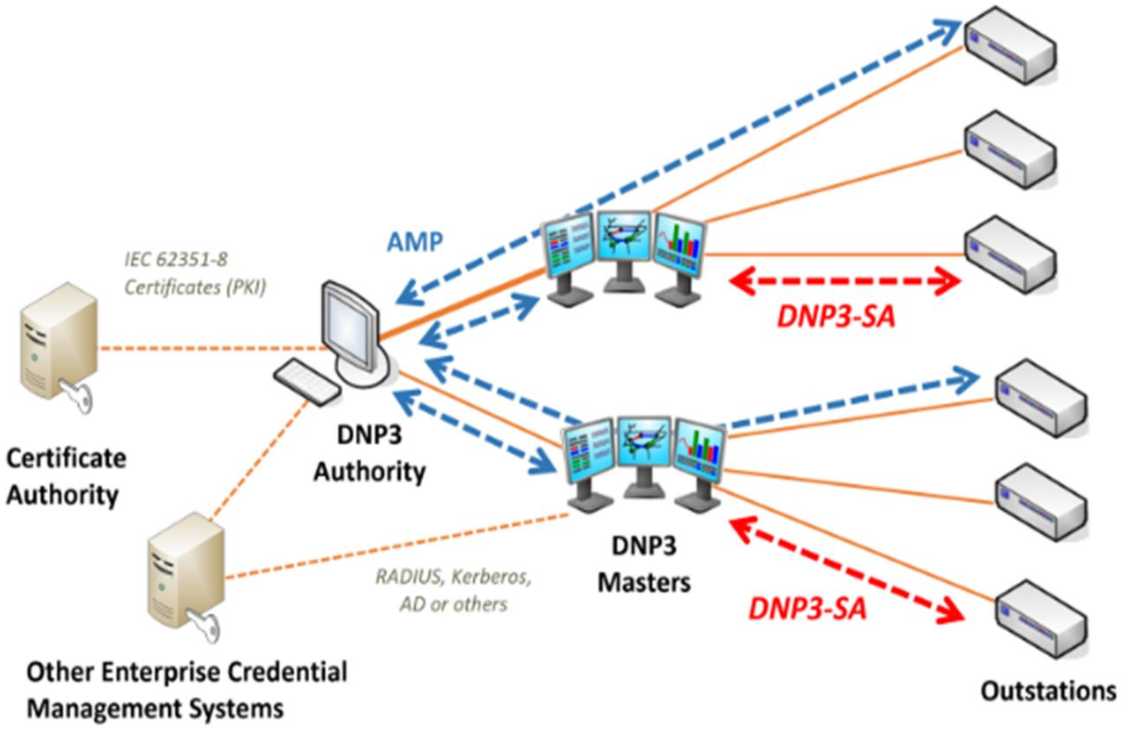

Data Link **Frame** (DLPDU)
Transport **Segment** (TPDU)
Security Session Protocol Data Unit (SPDU)
Application **Fragment** (APDU)
DNP3 Data Link Header
DNP3 Transport Header
DNP3-SA Header
DNP3 Application Header
DNP3 Object Headers and Objects
CRCs inserted

https://www.dnp.org/Portals/0/Public%20Documents/Overview%20of%20DNP3%20Security%20Version%206%202020-01-21.pdf?ver=YzjtxDEkBm15MV-vFJ-WDQ%3d%3d

DNP3 Secure Authentication (DNP3-SA)

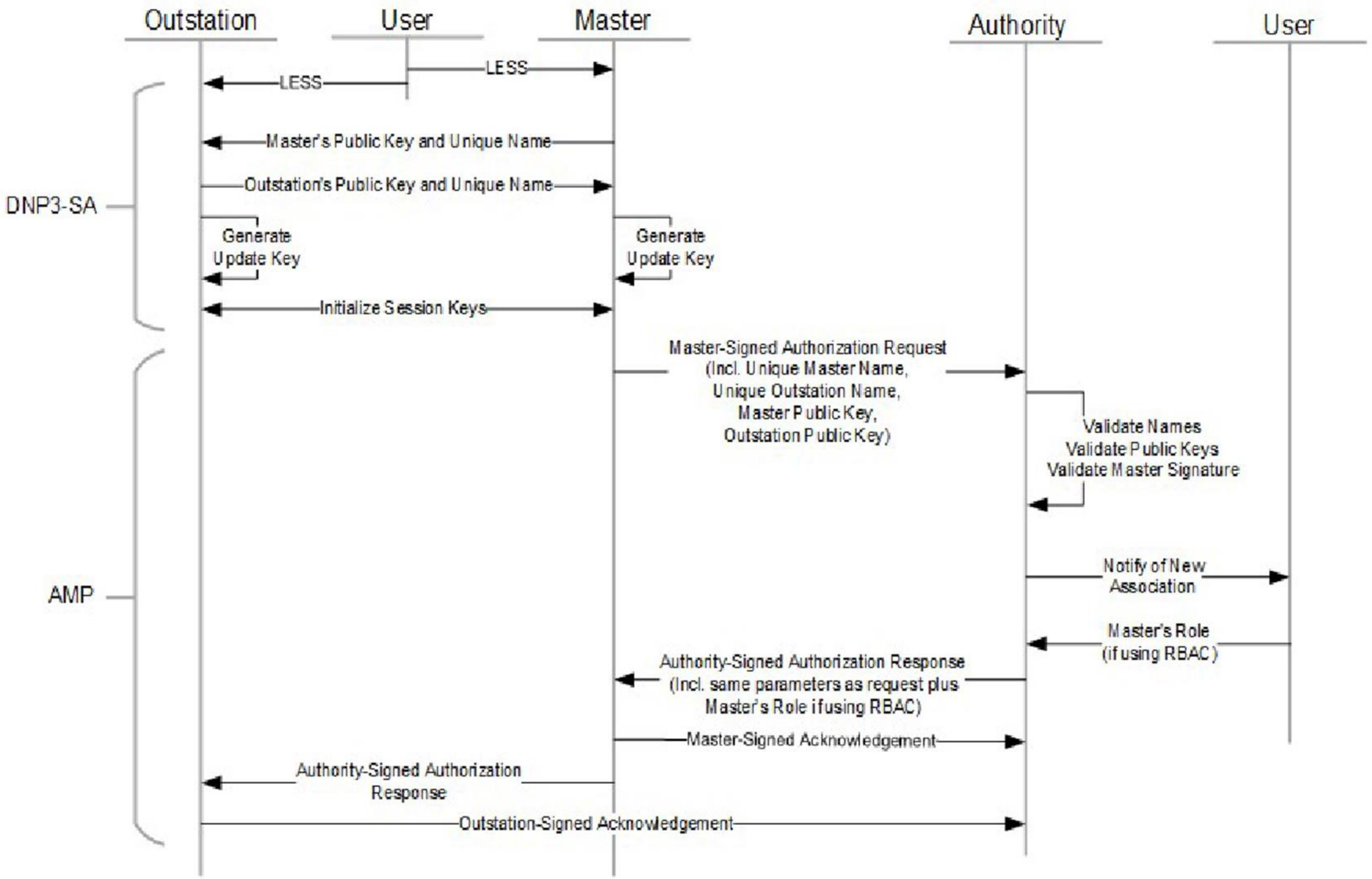


Authorization Management Protocol (AMP)



- DNP3 devices may not have access to network layer communications, AMP builds its own routing tables to direct messages between masters, outstations and a central Authority.

Enrollment and Authorization


Outstation
User
Master
Authority
User
LESS
LESS
DNP3-SA
Master's Public Key and Unique Name
Outstation's Public Key and Unique Name
Generate Update Key
Generate Update Key
Initialize Session Keys
AMP
Master-Signed Authorization Request (Incl. Unique Master Name, Unique Outstation Name, Master Public Key, Outstation Public Key)
Validate Names
Validate Public Keys
Validate Master Signature
Notify of New Association
Master's Role (if using RBAC)
Authority-Signed Authorization Response (Incl. same parameters as request plus Master's Role if using RBAC)
Master-Signed Acknowledgement
Authority-Signed Authorization Response
Outstation-Signed Acknowledgement

- A human user provides a Low-Entropy Shared Secret (LESS) essentially a one-time-use password, to approve and commission the communications between the two devices.

References

- https://instrumentationtools.com/dnp3-communication-protocol-overview/

- https://www.linkedin.com/advice/1/what-advantages-disadvantages-using-dnp3

- https://en.wikipedia.org/wiki/DNP3

- https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7947865

- Overview of DNP3 Security Version 6 https://www.dnp.org/Portals/0/Public%20Documents/Overview%20of%20DNP3%20Security%20Version%206%202020-01-21.pdf?ver=YzjtxDEkBm15MV-vFJ-WDQ%3d%3d

- https://www.dnp.org/Portals/0/Public%20Documents/SAv6%20and%20AMP%20flyer%20-%202022%20-%20Final.pdf?ver=z_i7KIkCzZDyYSWJPhU3KA%3d%3d