Distributed Network Protocol

Why IEEE 1815 (DNP3) Secure Authentication?

- Cyber-Security
  - End to end cryptographic authentication at the application layer which goes beyond VPN tunnels or TLS
  - Works end-to-end in mixed networks of IP and serial, including serial radios
  - Addresses threat of spoofing, modification, and replay of messages
  - Meets IEC 62351 security standard including Role Based Access Control (RBAC)

- Not encryption
  - TLS is supported for DNP3 IP based networks
  - Legacy support for networks or devices that do not support encryption
  - Clear messages (not encrypted) may be preferred in some systems

- Authentication of Critical Commands
  - Each critical operation is authenticated
  - Outstation may configure which requests are considered critical
  - Authentication can be performed in either direction (Outstation or Master)

- Multiple Users
  - Supports Role Based Access Control - multiple users and roles (engineers, operators, viewers, admin) which can be configured for organizational structure
  - Users can be added, modified, or removed from the system
  - Not just about cyber-security requirements but also to support utility operations
  - Role based access reduces risk that users unintentionally perform operations
  - Also supports multiple organizations that have different roles (view vs. operate)

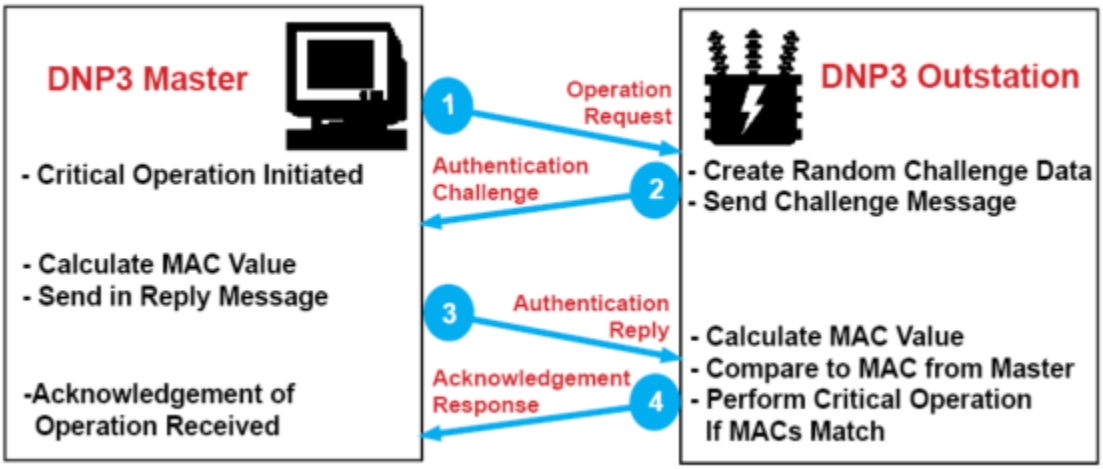
- Legacy Support
  - Support low bandwidth and/or serial networks
  - Low overhead for Outstations that may not have processing capability for public/private certificates or encryption
  - Allows upgrade path without requiring infrastructure or equipment upgrades

Benefits of DNP3 Secure Authentication

- End to end cyber-security at the application layer goes beyond TLS or VPN
- Security upgrade path without upgrading existing infrastructure or legacy devices
- Increased security and reliability with reduced risk of unintended operations
- Role Based Access Control allows utilities to enforce roles within their organization
- Can help meet authentication requirements of NERC CIP

Benefits of DNP3 Remote Key Management

- Add, remove, or modify users as organization changes or when user leaves organization
- Reduced cost to update keys in remote devices (no truck rolls)
- Change keys quickly after an unintended key disclosure
- Reduced risk of key disclosure versus manual distribution



Distributed Network Protocol