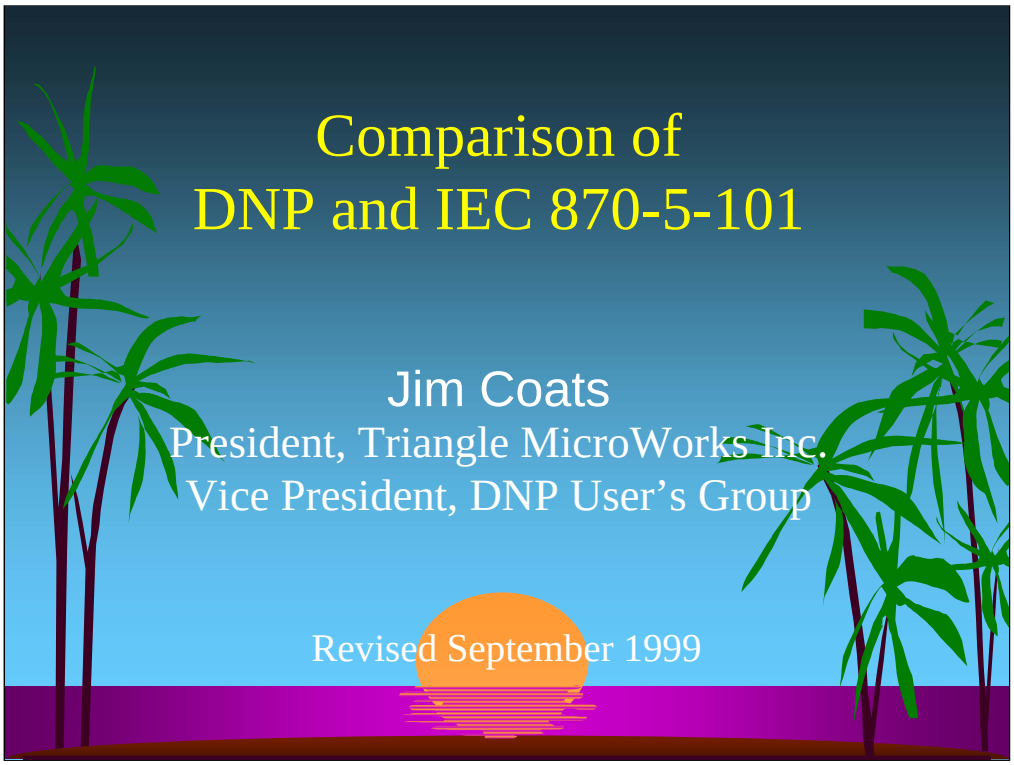
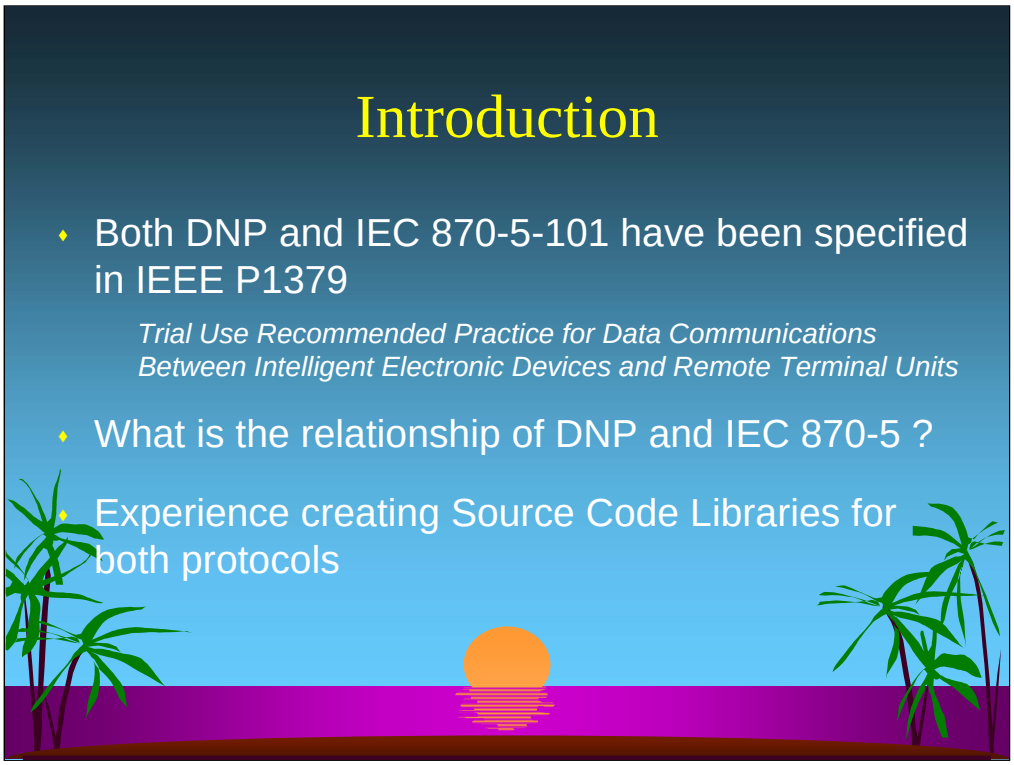
This presentation was originally prepared for the January 1997 meeting of the DNP Users Group.

It has been revised to clarify ambiguous items; in response to comments received from industry experts; and to reflect recent changes in the respective protocols descriptions and items under review by the IEC and DNP Technical Committees.

Andrew West

15th September, 1999


Comparison of
DNP and IEC 870-5-101
Jim Coats
President, Triangle MicroWorks Inc.
Vice President, DNP User's Group
Revised September 1999



Is DNP Based on IEC 870-5?

DNP's framing is based on (but not identical to) a framing format specified in 870-5-2. The application layer is not based on any of the 870 standards. DNP was specified soon after 870-5-2 was published, before the 870-5-4, -5 and -101 application standards were published.

Is DNP IEC 870-5 compliant?

No.

Both protocols provide similar application functionality.

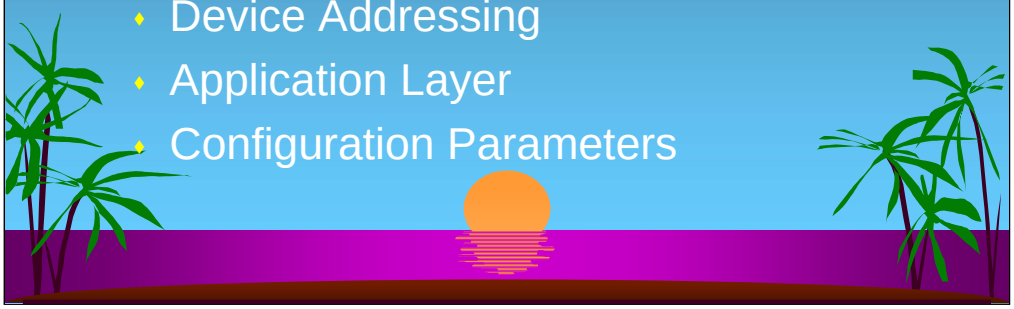
They were primarily designed for point-to-point or multi-drop serial link architectures, but can work over radio, LAN, etc.

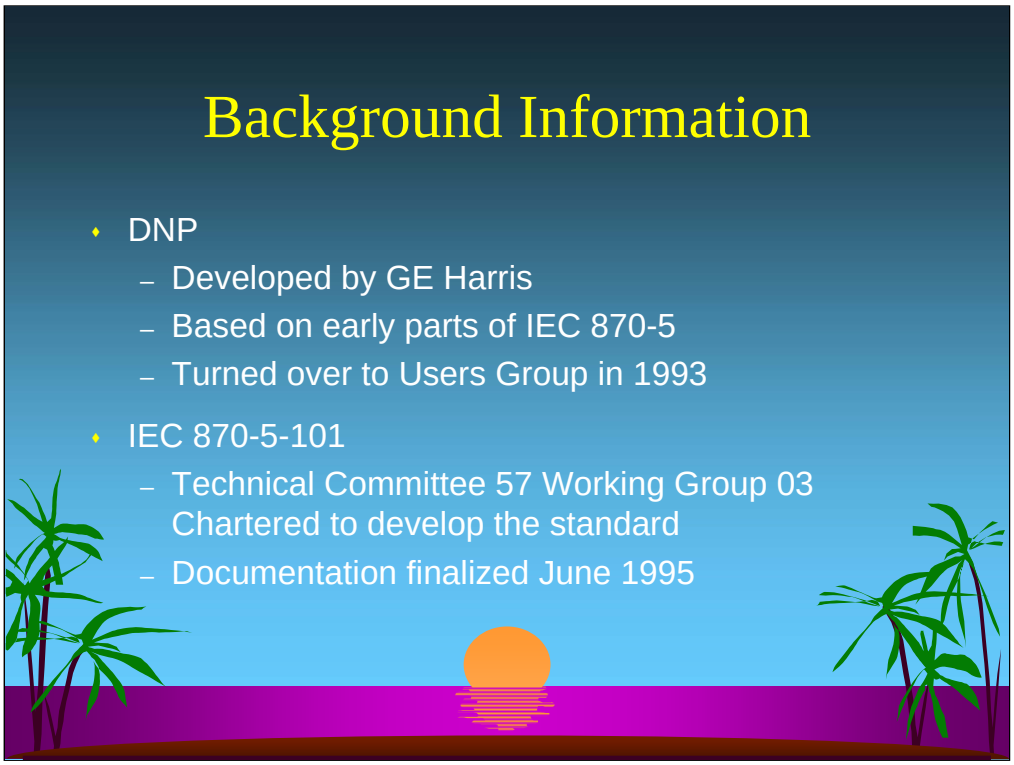
Both protocols are used worldwide for electric power SCADA. DNP is dominant in North America, Australia, South Africa. IEC is required by legislation in some European countries. It is also common in the Middle East. In most of Asia and South America both are used almost equally.

DNP has gained wide acceptance in non-electric power applications, where IEC is little used.

Agenda

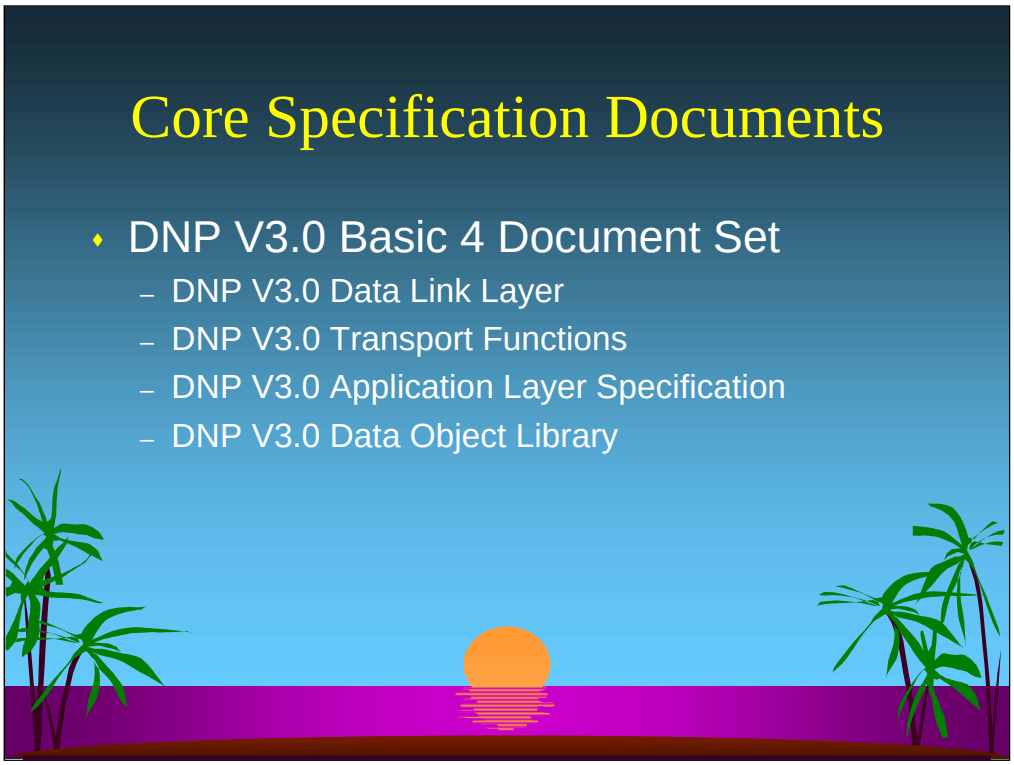
- Background Information
- Protocol Specifications
- Data Link
  - Balanced
  - Unbalanced
- Device Addressing
- Application Layer
- Configuration Parameters



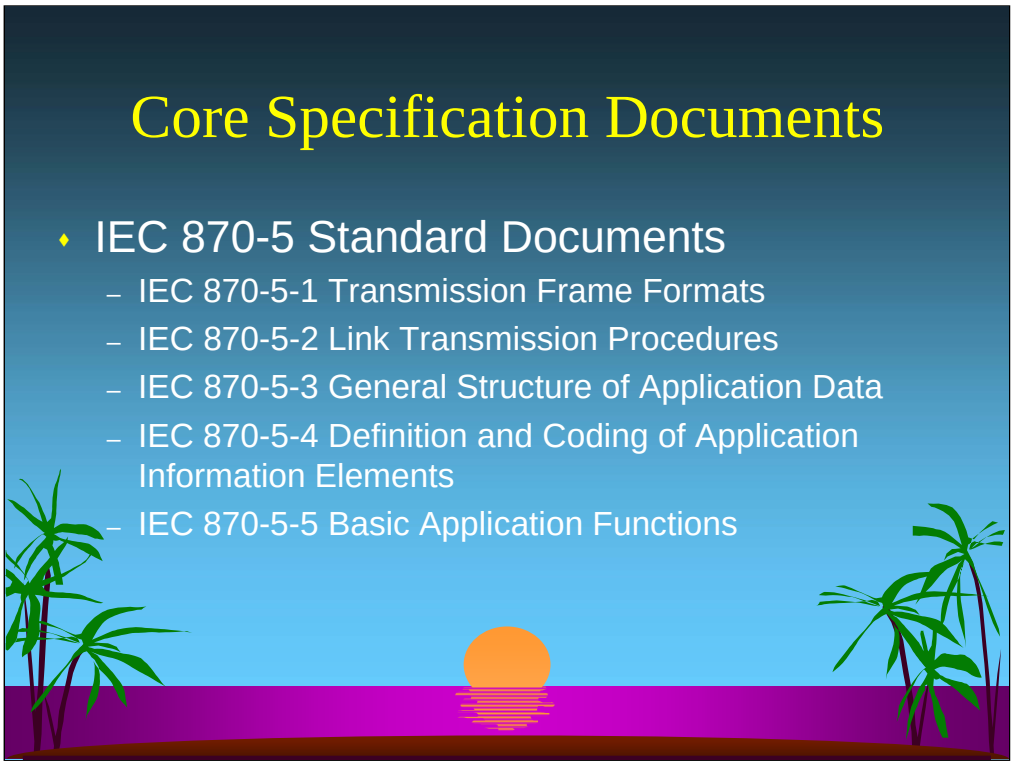


•DNP continues to be expanded by the addition of new objects, under the guidance of the DNP Technical Committee.

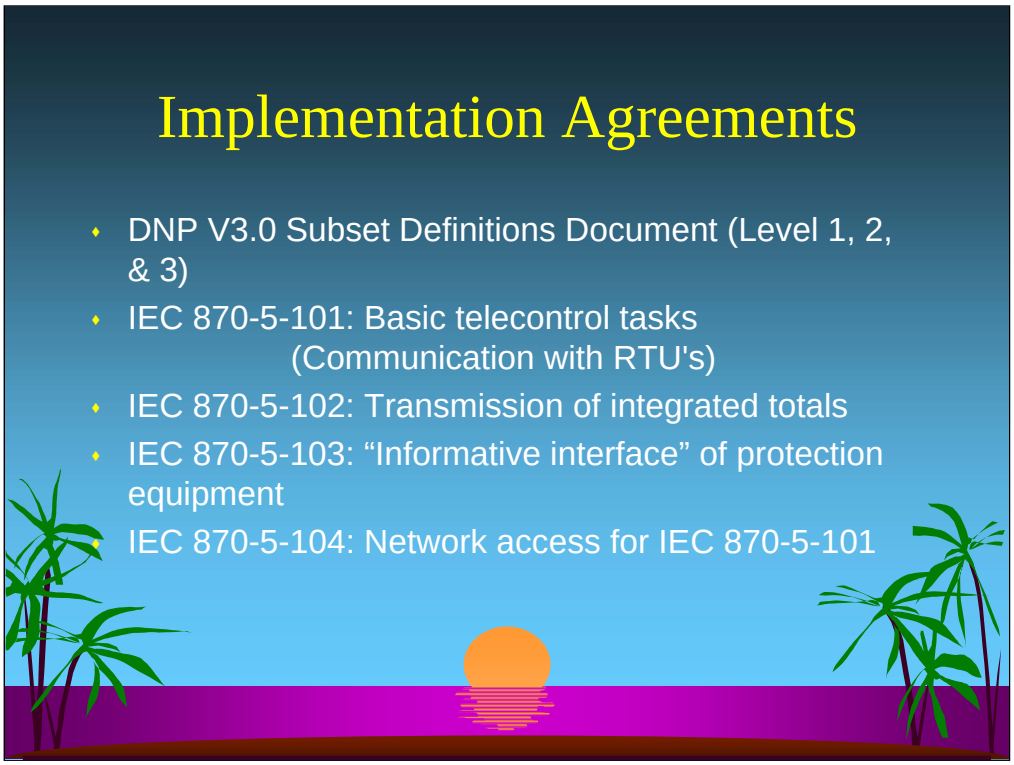
•IEC 870-5-101 has been expanded with new objects to transport more-complete time tags. Further amendments are in production by the IEC Working Group.



The DNP Basic 4 document set is augmented by a Subset Definition document, a number of Technical Bulletins and Conformance Test Procedures. All of these documents are available for download by DNP User Group members from the DNP web site.



The IEC standards may be purchased directly from the IEC in Switzerland, or from the national standards bodies in most countries. The documents can be downloaded from the IEC web site.



IEC 870-5-101: published November 1995

IEC 870-5-102: published June 96

IEC 870-5-103: published December 1997

IEC 870-5-104: CDV February 1999

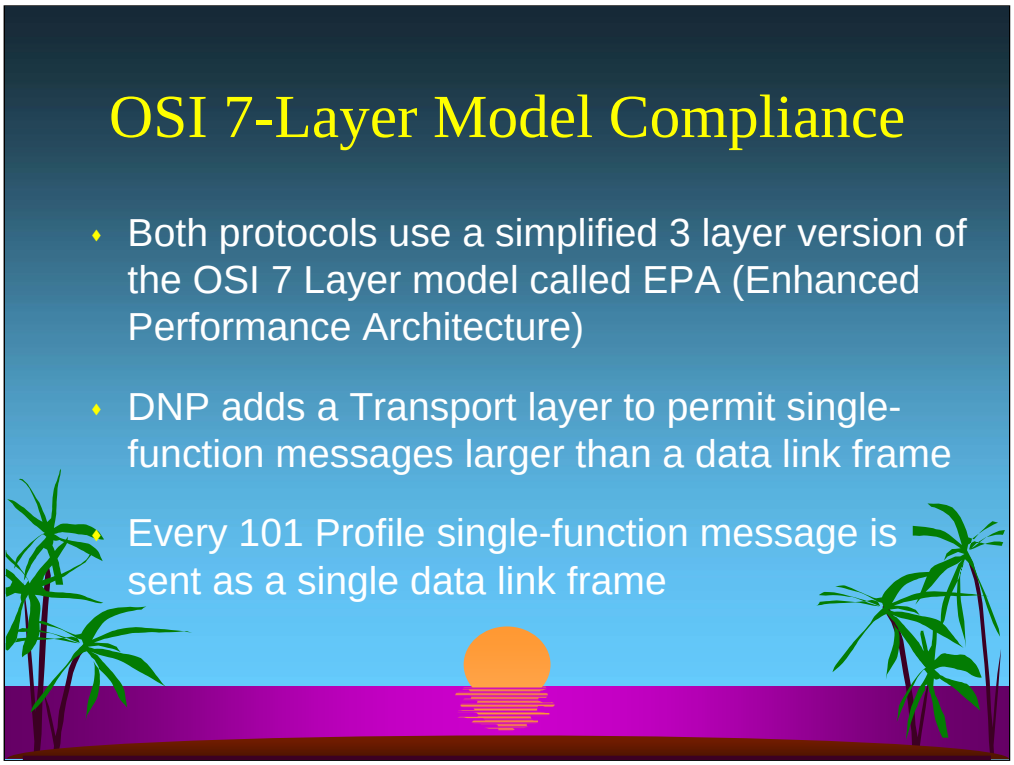
104: The ASDU's from IEC 870-5-101 are used, but the lower layers are based on standard transport profiles

101:Addendum adding new time-tag formats for event objects (RVC November 1998), addendum with supplementary definitions in preparation.

The 101, 102 and 103 profiles are essentially separate application protocols that have common design elements.

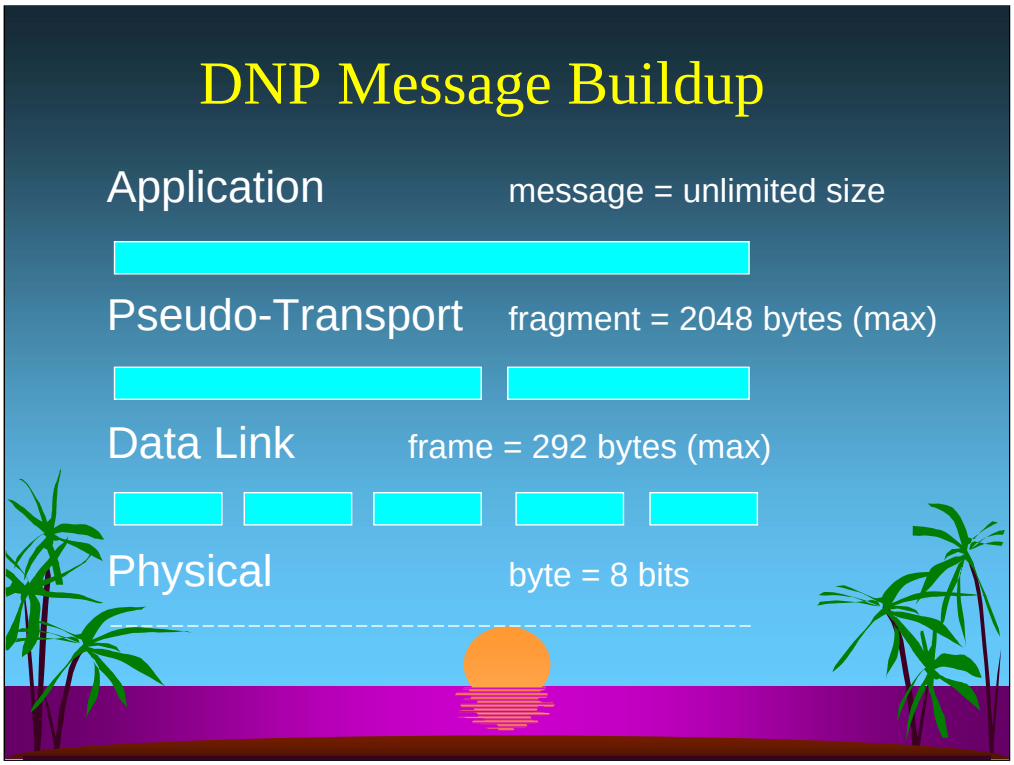
An interoperability checklist is used in 101 to identify the protocol subset supported by a device.

DNP specifies Subset Levels and a device profile document to identify interoperability between devices.



In DNP all application layer functions are implemented as application layer messages encapsulated in data link frames.

101 supports a mechanism to specify a set of application functions (e.g. poll requests) in a data link layer message containing no application data. This improves efficiency, but blurs the separation of application and data link functionality.

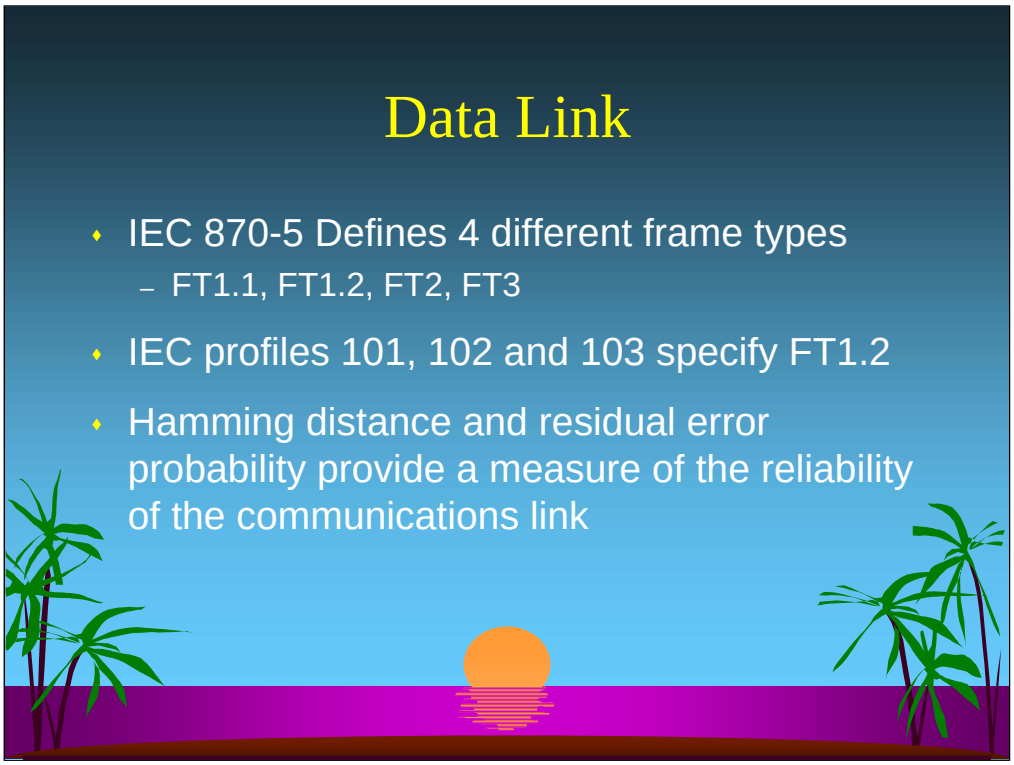


•Receive goes up the stack, transmit goes down the stack.

•Size of data transmitted/received may fit into one data link frame. So do not require multi-frame fragments or multi-fragment messages.

•A single DNP application function is usually sent as a single application layer message, which can consist of many data link frames.

•IEC 870-5 has no transport layer. Each data link frame containing application data is a complete application message. A single application function (e.g.: interrogation) may require that several messages are sent to complete the function.



Major differences between frame formats

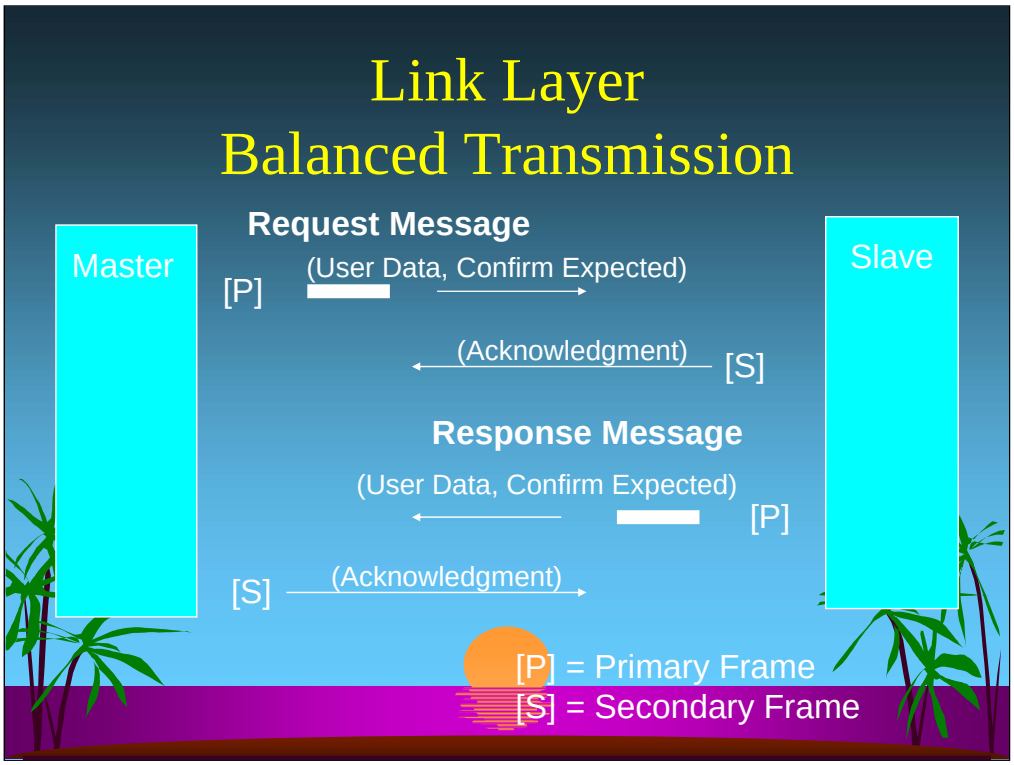
Address size and format for source and destination are specified in DNP, a single address size is selected from several options in 101.

DNP only uses variable-length frames. IEC 870-5-101 uses single character ACK, fixed-length frames and variable-length frames.

Hamming distance is the number of single bit errors which must occur for a corrupted message to be mistaken for a valid message

IEC 870-5 Frame Type Comparison

Frame Type	Hamming Distance	Security	Max Length
FT1.1	2	Even Parity	128
FT1.2	4	8 bit Checksum	255
FT2	4	8 bit CRC	255
FT3	6	16 bit CRC	255

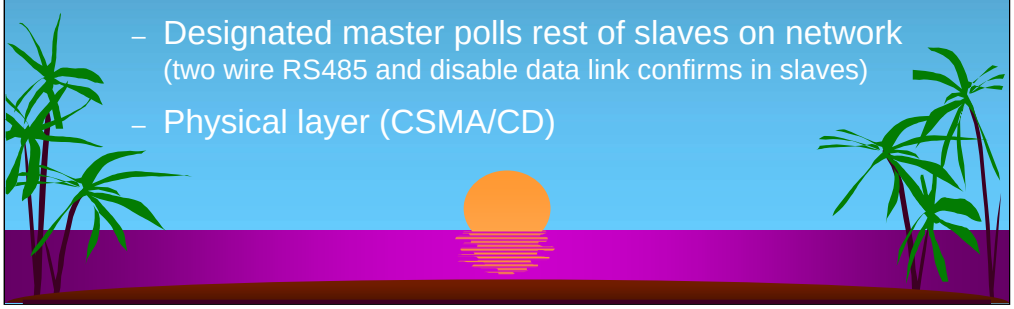


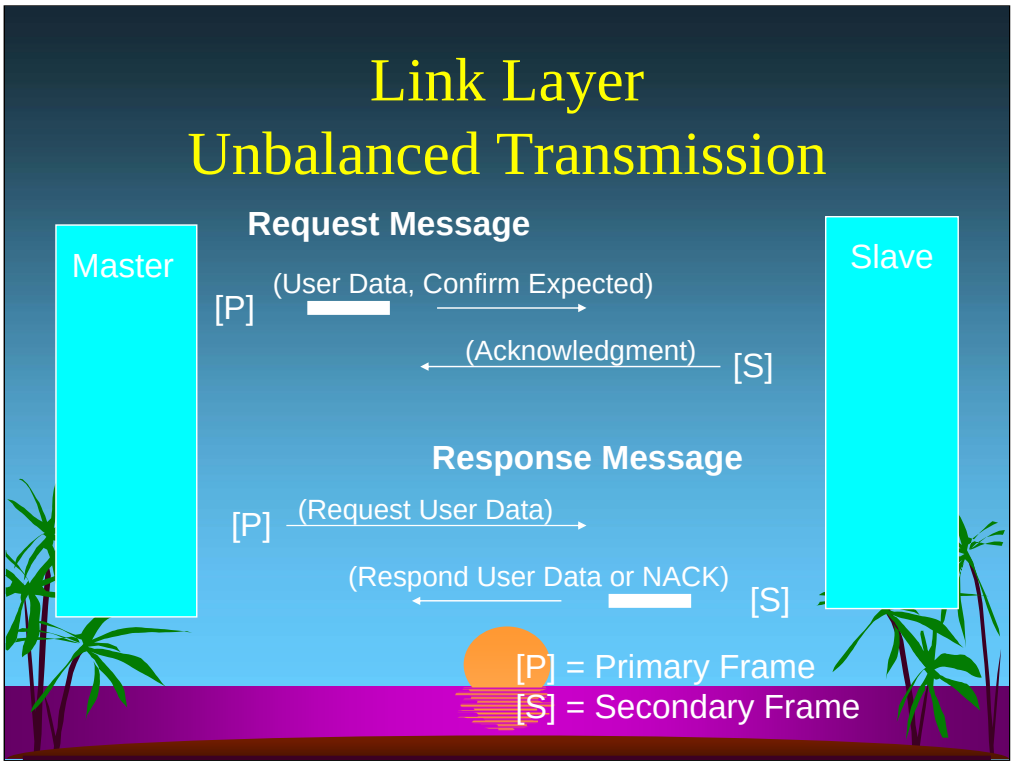
DNP only uses balanced transmission

IEC profiles permit either balanced or unbalanced transmission

Link Layer
Balanced Transmission

- At the link layer, all devices are equal
- Collision avoidance by one of the following:
  - Full duplex point to point connection (RS232 or four wire RS485)
  - Designated master polls rest of slaves on network (two wire RS485 and disable data link confirms in slaves)
  - Physical layer (CSMA/CD)

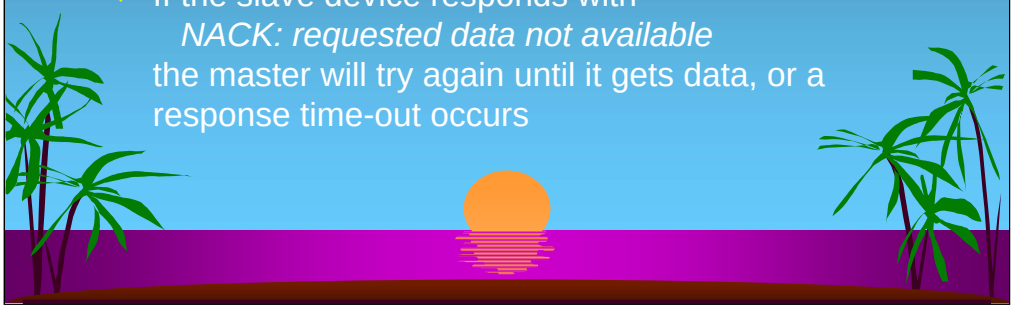


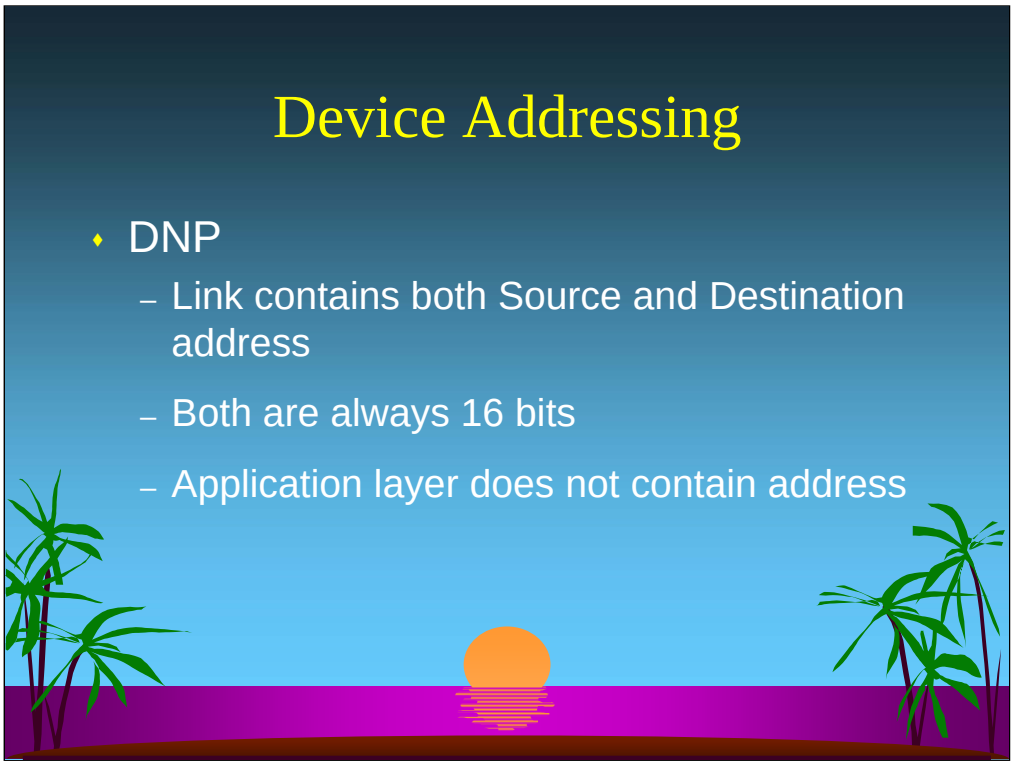


Not supported in DNP

Link Layer
Unbalanced Transmission

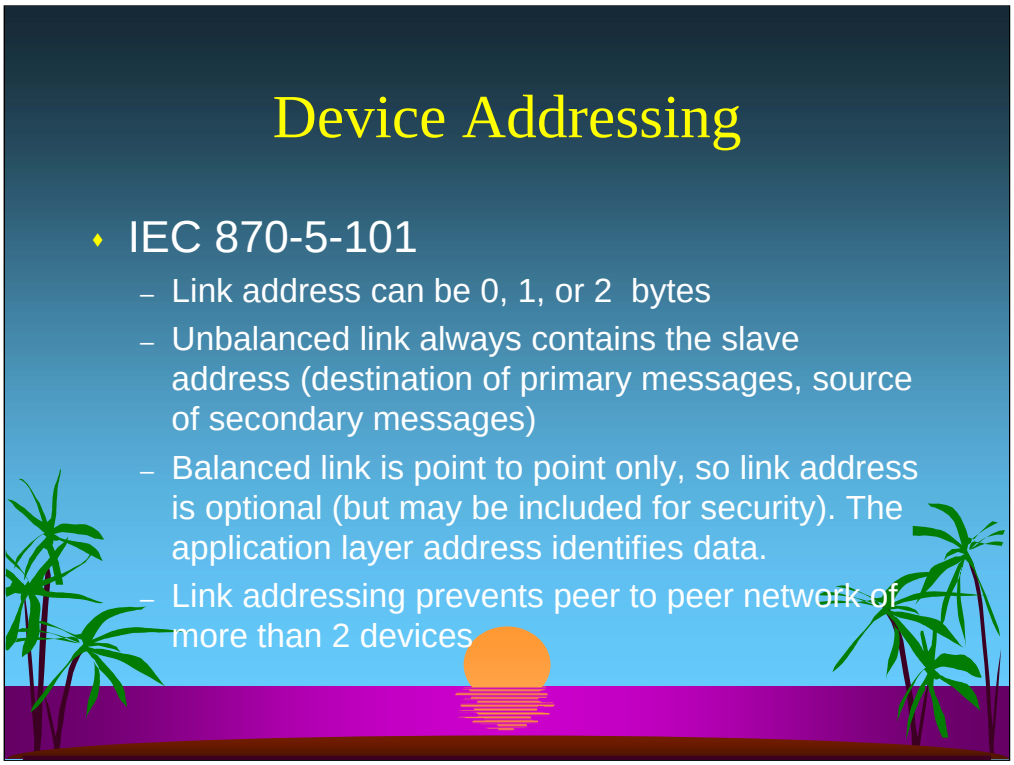
- Only Master device can transmit primary frames
- Collision avoidance is not necessary since slave device cannot initiate exchange, or retry failed messages
- If the slave device responds with
  NACK: requested data not available
  the master will try again until it gets data, or a response time-out occurs





The provision of a source and destination address simplifies message routing in certain network topologies.

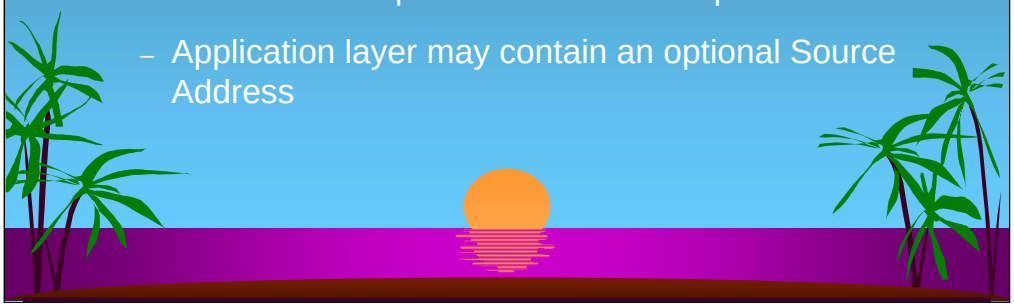
A DNP link address is a device's logical address. A single physical device is permitted to respond to multiple addresses (contain multiple logical devices). Each device will appear to the master as a completely separate device.

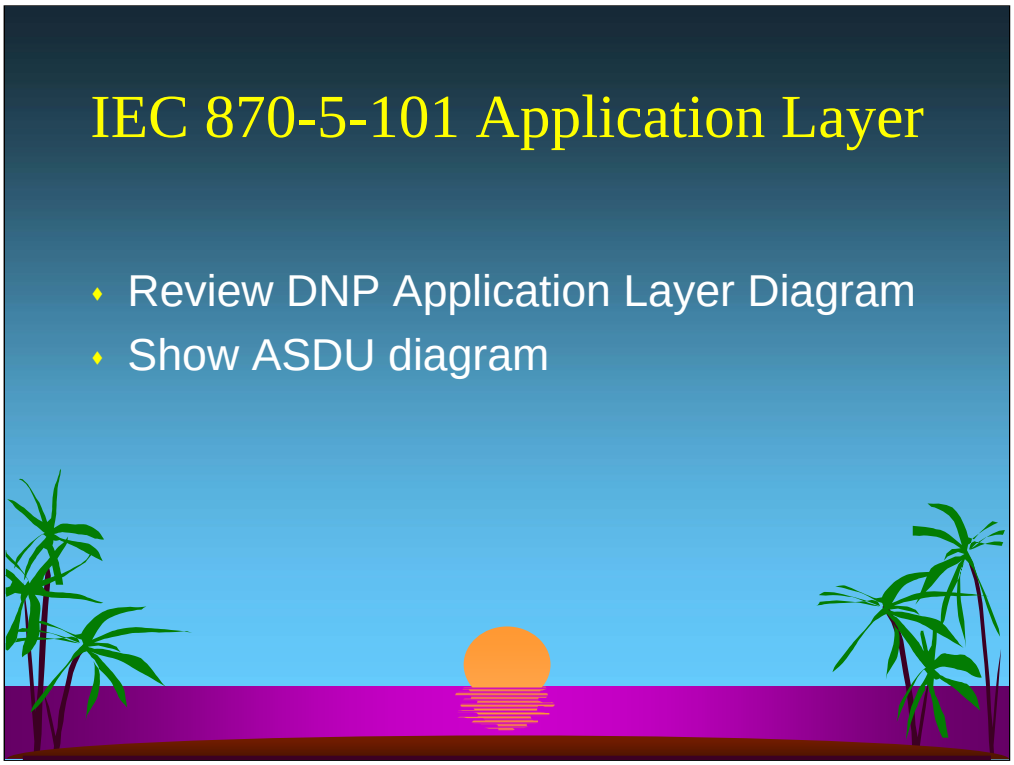


The DNP concept of “peer-to-peer” operation where pairs of devices may swap “master” and “slave” roles does not appear to have a parallel in the IEC profiles.

Device Addressing

- IEC 870-5-101 (continued)
  - Application layer *sector address* (common address of ASDU) can be unrelated to link address of device
  - Can have multiple *sector addresses* per device
  - Application layer may contain an optional Source Address





Type ID - Identifies the object format

Qualifier

- Quantity of points
- indexed or sequence of points

Cause of Transmission - optional originator address

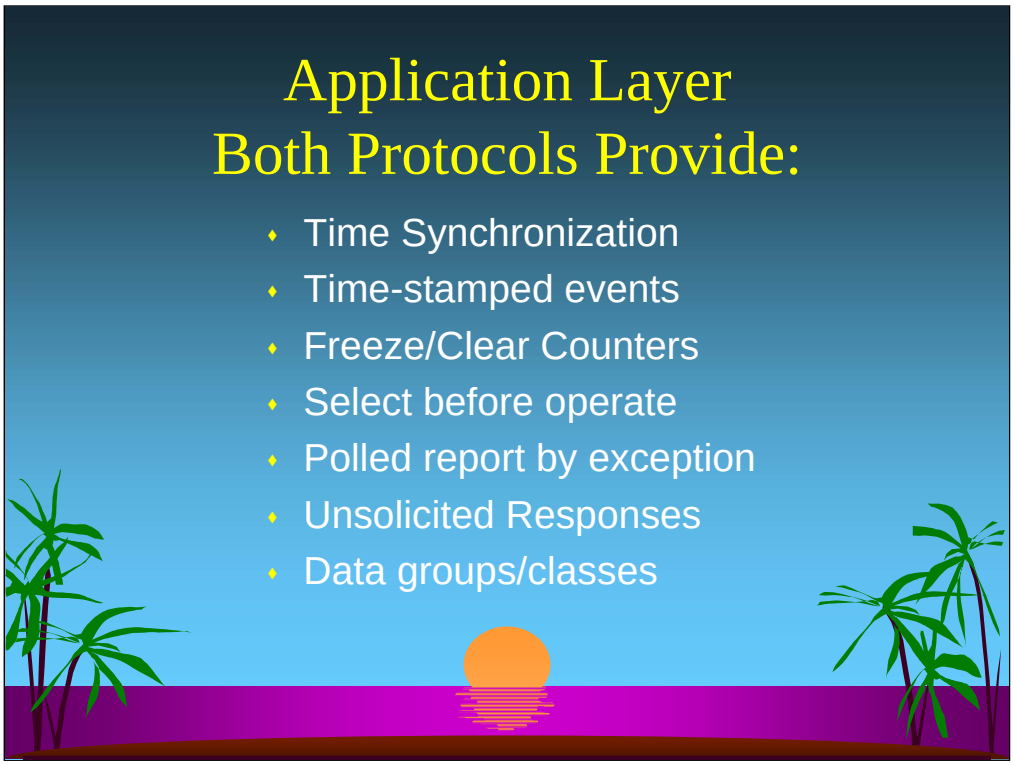
- e.g.: cyclic; spontaneous; activation; activation termination

ASDU Address - 8 or 16 bits fixed

Information Object Address - 8, 16, or 24 bits fixed

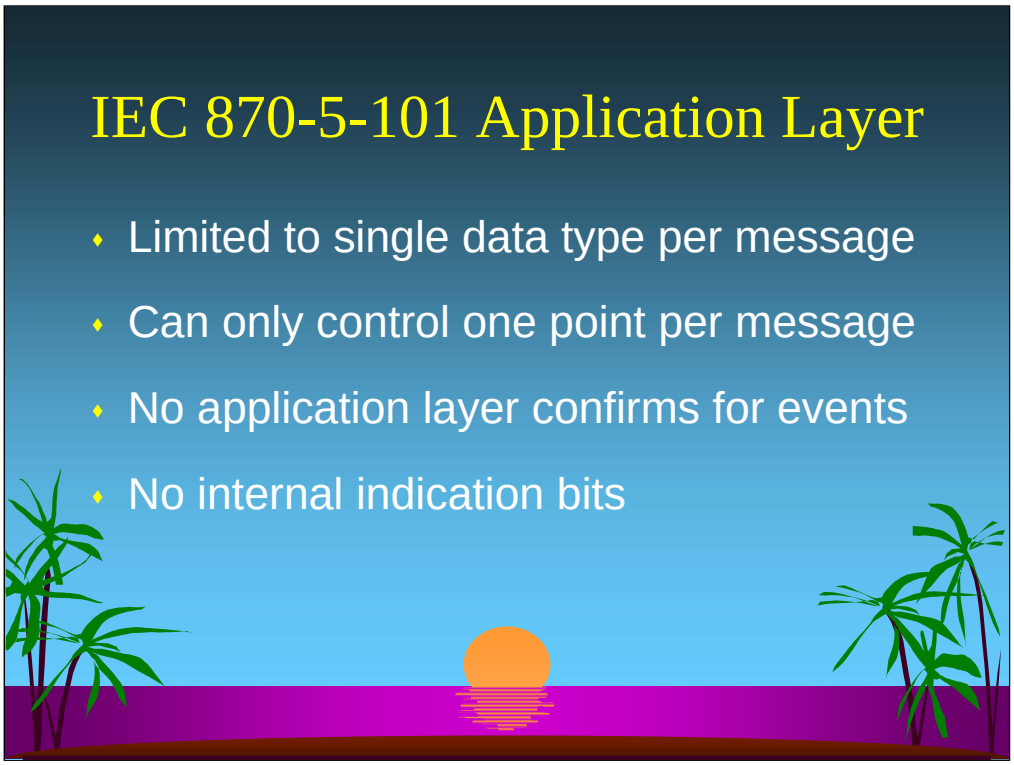
- Point number - repeated if qualifier is indexed

Data - repeated *quantity* times



End result of application layer is very similar

Different means to accomplish same task



DNP permits multiple data types in one message. 101 requires one data type per message.

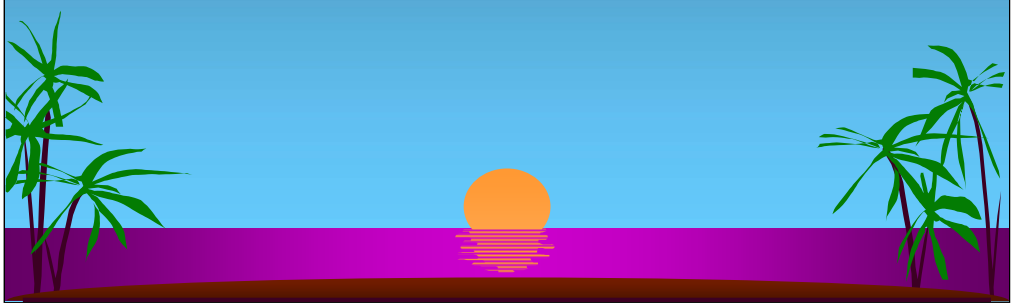
DNP permits multiple points to be controlled in one message transaction sequence (e.g. select/execute). 101 requires a separate transaction sequence for each control point.

DNP relies on an application layer confirm to guarantee the master has received events before clearing them from an event buffer. 101 relies on the security features of the data link layer.

DNP defines specific indications. 101 relies on configuring of particular process variables as indications to provide any necessary functions.

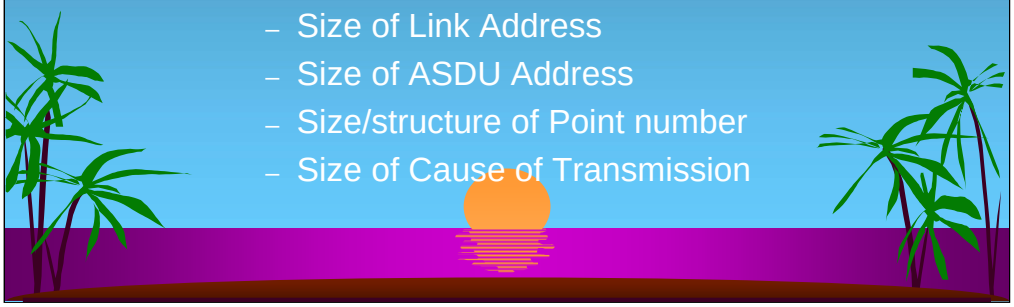
Configuration Parameters Required for Basic Communication

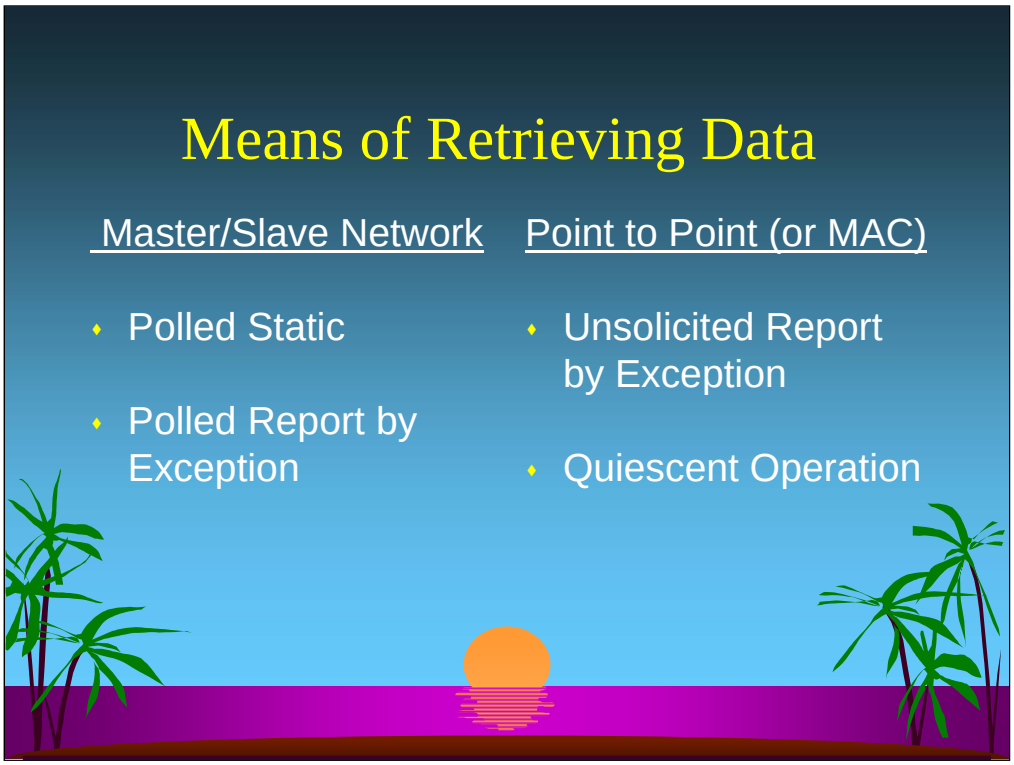
- DNP
  - Baud Rate
  - Device Address
  - Fragment Size



Configuration Parameters Required for Basic Communication

- IEC 870-5-101
  - Baud Rate
  - Device Address
  - Balanced/Unbalanced
  - Frame Length
  - Size of Link Address
  - Size of ASDU Address
  - Size/structure of Point number
  - Size of Cause of Transmission





Master/Slave Network - Slaves do not speak unless spoken to

MAC = Media Access Control - CSMA/CD

Polled Static - Class 0 or specific data request message sent to each device

Polled Report by Exception - Class 1, 2, 3 request message sent to each device with occasional integrity (class 0) data poll.

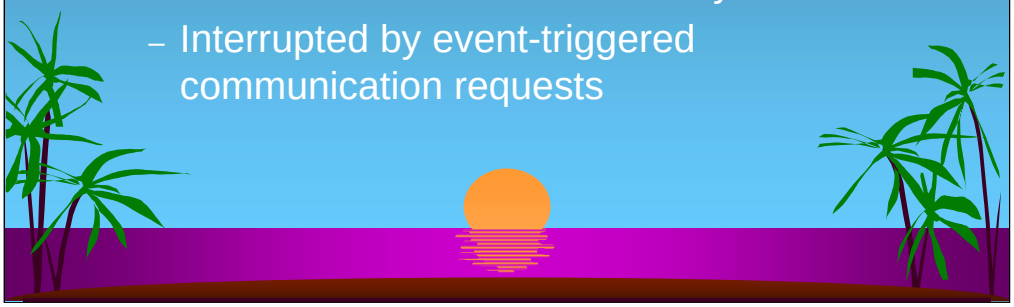
Unsolicited Report by Exception - most communication is unsolicited, but the Master occasionally sends integrity polls for class 0 Data to verify its' database.

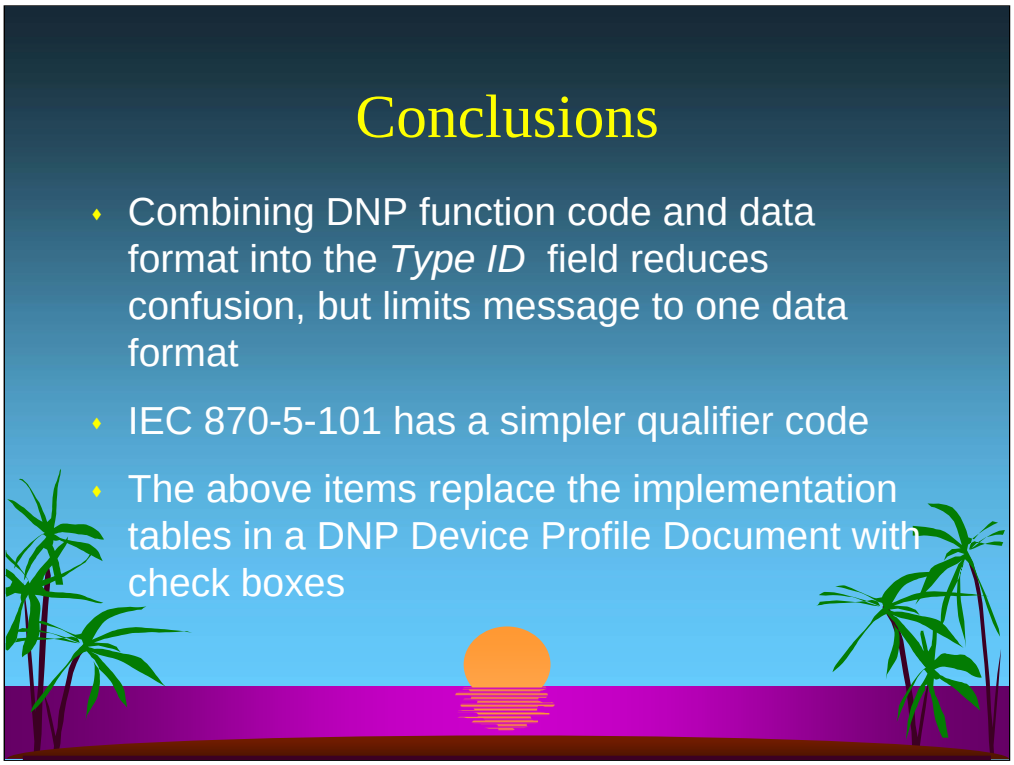
Quiescent Operation - master never polls slave

Last two modes are useful when communication medium is dial-up modem.

Additional IEC 870-5 Data Acquisition Methods

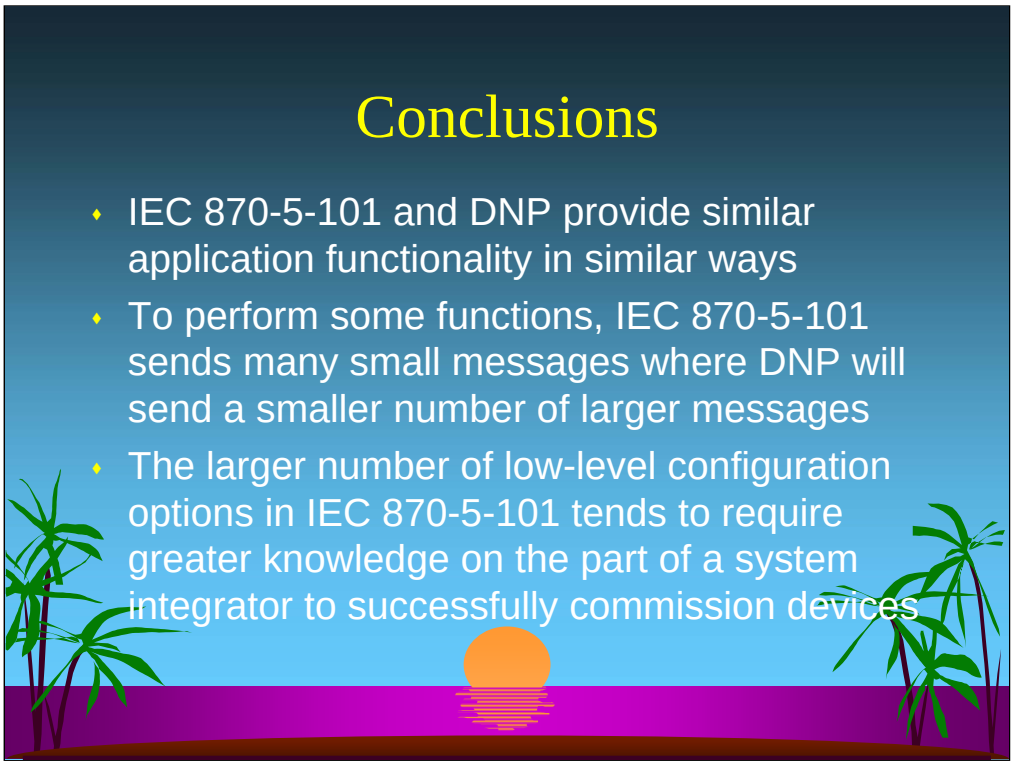
- Cyclic Data Transmission
  - Eliminates static data poll message from master
  - Balanced or unbalanced link layer
  - Interrupted by event-triggered communication requests





Because DNP permits multiple object types per message, it also requires a more complex object header format.

IEC uses a combination of Cause of Transmission and qualifier codes embedded in data objects (Type ID) in a similar manner to DNP's use of application function codes. DNP function code applies to all object types in the message.



More options in IEC typically means either more configuration options and support program code or else unsupported options so some IEC 870-5-101 devices do not communicate with other devices.

But: familiarity with one protocol makes the other look more complex, no matter which protocol is more familiar! Each has features that are elegant and simple, and features that are complex.

No technical support provided directly by IEC: questions are usually handled by consultants, vendors or volunteers who may contribute to the mail lists.

DNP technical support is provided by the DNP Technical Committee. DNP User Group members are automatically enrolled on a DNP mail list forum. Technical questions can be submitted to this list.