



Global Expert Conference 2019

OPC UA Wireshark Trace Analysis (Topic-no.: S16)



Goals

- Look at most common OPC UA services
- What information can be found
- Getting you more comfortable with OPC UA packets
- Giving tips for WS filter settings
- Analysis of a real problem



Time	Topic	Presenter
5min	Preparations	
10min	Capture 1st Wireshark trace of an OPC UA connection	
60min	Wireshark profiles and filter settings	
20min	Exercise – OPC UA Connect / Disconnect	
5min	Exercise – Encrypted WS Trace	
20min	Exercise – OPC UA Read / Write	
20min	Exercise – OPC UA Subscriptions	
30min	Exercise – SIEMENS Subscription problem	



Why Wireshark trace of OPC UA communication

- OPC UA open standard
- Different client / server implementations
- Difficult having them all
- OPC UA Binary protocol as basis



Network Topology

HUB:

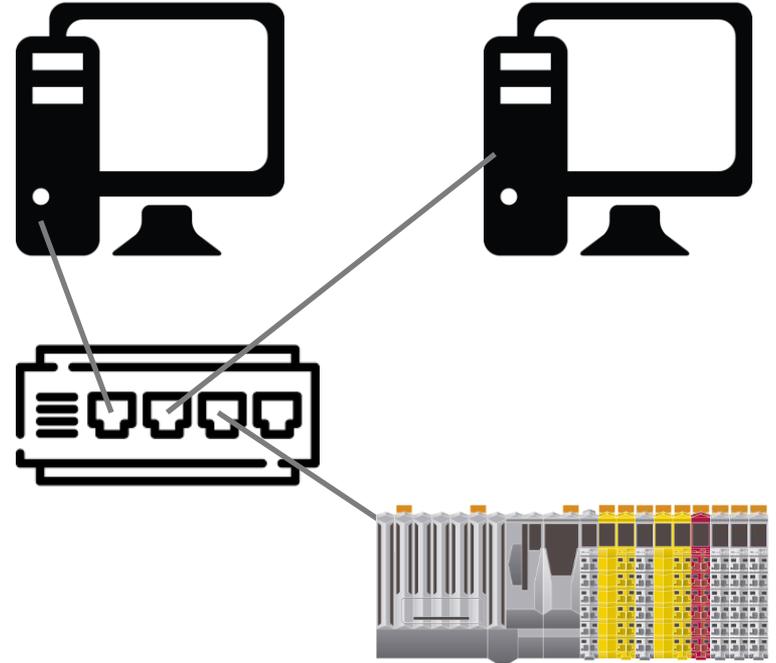
- Easiest possibility
 - Network traffic on all ports

Switch (unmanaged):

- Not possible
 - Network traffic only through respective port

Switch (managed):

- Possible
 - Network traffic can be configured for the ports





Exercise – OPC UA Connect / Disconnect

Open Excel file: **Exercise – Connect Disconnect.xlsx**

Open WS trace: **WS_ConnectDisconnect.pcapng**

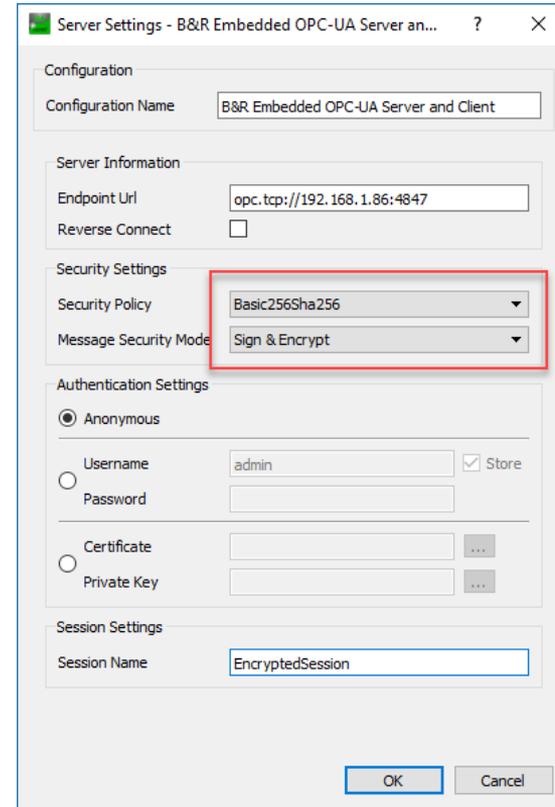
Find the information in the Wireshark trace

Time: 20min



Exercise – Capture WS trace of encrypted OPC UA connection

1. Select ETH IF and start WS trace
2. Connect with UA Expert to the OPC UA server
3. Disconnect from the OPC UA server
4. Stop the WS trace





Exercise – Read Write

Open Excel file: **Exercise – Read Write.xlsx**

Open WS trace: **WS_ReadWrite.pcapng**

Find the information in the Wireshark trace

Time: 20min



Exercise - Subscription

Open Excel file: **Exercise – Subscription.xlsx**

Open WS trace: **WS_Subscriptions.pcapng**

Find the information in the Wireshark trace

Time: 20min



Exercise – Methods

Open Excel file: **Exercise – Methods.xlsx**

Open WS trace: **WS_Methods.pcapng**

Find the information in the Wireshark trace

Time: 15min



Browse Path example

/NamespaceIndex:BrowseName ...

/0:Root

/0:Objects

/4:PLC

/4:Modules

/6:&:&: (ApplicationModule::Task:PV)

/6:ServerTask

/6:LightOn

/0:Root/0:Objects/4:PLC/4:Modules/6:&:&:/6:ServerTask/6:LightOn



Exercise – Any Device Connection

Open Excel file: **Exercise – Any Device.xlsx**

Open WS trace: **WS_AnyDevice.pcapng**

Find the information in the Wireshark trace

Time: 20min



Exercise – SIEMENS Subscription Problem

Problem:

We are trying to read data via OPC UA from a Siemens S7 but since we need the data cyclically we want create a subscription to this variable.

All connection is fine and we can also successfully read the item a single time with a read request.

However if we try to create a subscription an error appears:

OpcUa_BadNodeIdUnknown 0x80340000 The node ID refers to a node that does not exist in the server's address space.

Server Port: 4840

Server IP: 172.16.0.1 // Client IP: 172.16.0.55



Thank you for your attention.

OPC UA Wireshark Trace Analysis