Introduction to Baselining the Ethernet Traffic of Substation Communication Networks

Dr. Xiaoguang Ma  
ABB Inc.  
Lake Mary, USA  
xiaoguang.ma@us.abb.com

Wei Huang  
ABB Inc.  
Lake Mary, USA  
Wei.huang@us.abb.com

Abstract—With the development of modern communication technologies and new communication protocols, e.g., the seamless redundancy protocol HSR/PRP, the IEEE 1588v2 (PTP), and IEC 61850, the communication network plays a more important role in current relay applications, such as the automatic transfer switch (ATS) application, the communication-assisted protection schemes and the sample measurement values (SMV). Therefore setting up and maintaining reliable Substation Communication Networks (SCN) becomes a critical issue for the grid operator.

This paper introduces the process of maintaining and inspecting the communication baseline of the SCN to help to prevent communication failure, detecting intrusion and expediting troubleshooting.

In this paper, the Open Systems Interconnection (OSI) model is employed. The requirement of basic understanding of Ethernet protocols (e.g. ICMP, TCP and IP), commands (e.g. ping, tracert) and hardware and software tools (e.g. the nTAP and the Wireshark) is also discussed.

Index Terms— Baseline, Ethernet, OSI, TCPIP.

I. INTRODUCTION

With the development of the industrial communication network, new infrastructures, including wired and wireless Ethernet communication, redundancy communication, and new protocols, e.g. the IEC 61850, IEEE 1588 (PTP) v2, bring more challenge to maintain and troubleshooting in the SCADA Communication Network (SCN). Even more complicated, in some scenario the coexistence of modern and legacy communication, e.g. the serial communication, makes it extremely hard to find, “the needle in the hay”, which part of the communication path is broken. There are sophisticated network diagnosis and analysis service provided in the market. However, for the security, privacy or cost concerns, a lot of users would prefer to perform the diagnosis and analysis by themselves, especially considering that the particular industrial protocols and communication structures may introduce a steep learning curve to the third-party network service providers. In this paper, we only introduce some basic cost effective methods to network diagnosis and analysis before resorting to costly third-party services.

In this paper, the Open Systems Interconnection (OSI) model is employed to help to locate and to isolate the communication issue.

The top communication issues customers raised are:
1) General communication interruption.
2) Specific protocol doesn’t work as expected
3) Missing data from specific protocol

The first issue is mostly resident in the first three layers of the seven layer OSI layer model, i.e. physical layer, the data link layer (MAC) and the network layer (IP). The second issue is more related to Layer 3 and up, i.e., the network layer, transport layer (TCP/UDP), the session layer, the presentation layer and the application layer. The last issue is mostly caused by the application layer.

The baselining will provide most values for the lower 4 layers, while the top layer is mostly affected by the system or application configuration.

In rest of the paper is organized as follows. The section II will introduce the OSI model and basic issues. The hardware and software of baselining will be introduced in section III. A common troubleshooting with established baseline will be lined out in section IV.

II. OSI MODELS AND TYPICAL ISSUES

A. Physical Layer

This layer defines physical characteristics of connection methods, e.g., the RJ45 cable, fiber optics or wireless, and connectors, and provides the interface between network and network devices.

Some typical physical layer issues can be easily identified by high lost package rate, e.g. an unplugged RJ45 cable, an
unmatched pair of fiber cable and receiver, heavily interfered wireless communication channel, etc.

B. Data Link Layer
The data link layer is normally represented by a Layer 2 switch, includes MAC sub layer and LLC sub layer. The HSR/PRP redundancy protocols are implemented in this layer. The LAN management protocols work in this layer, including MRP, RSTP, etc. Some popular LAN communication protocols are also directly built on this layer, e.g., the GOOSE, SMV, PTPv2 over Ethernet with power profile.

Some industrial communication protocols are directly built on this layer and employ broadcast address in this layer. For example, GOOSE use 01-0C-CD-01-00-00 to 01-0C-CD-01-01-FF, SMV use 01-0C-CD-04-00-00 to 01-0C-CD-04-01-FF and PTPv2 over Ethernet use 01-1B-19-00-00-00 for Announce, Sync and Sync Follow_Up messages, or 01-80-C2-00-00-0E for peer-to-peer Delay Req and Resp messages. For security reason, some router will block certain broadcast address. It is important to ensure those broadcast messages can be delivered to all destination ports.

VLAN configuration also needs to be checked to ensure the sender and targeted receivers are in the same VLAN group.

C. Network Layer
The network layer is also called IP layer and represented by a Layer 3 router or switch, with the functionality of logical addressing, routing, and packet generation.

In this layer, most issues are caused by misconfiguration of the unit’s IP address, subnet mask, or default gateway, or blocked service port.

D. Transport Layer
The transport layer is responsible for building and maintaining sessions between devices, it serves to connect the lower layers (1-3) to the higher layers (5-7). The transport layer enables end-to-end connection and connectionless data delivery management, ensures reliable packet delivery caused by network congestion and errors.

The prevailing protocols run on this layer are the TCP and the UDP. The TCP three-way handshake process offers critical network diagnostic information. For example, if multiple SYNs are sent by no SYN-ACK are received, this is normally caused by an unstable communication link, high packet loss rate is hinted, or SYNs packets are followed by RST packets shows application layer rejection of the conversation.

Observing the round trip time between the SYN and SYN-ACK offers the shortest response time between the client and the server since this conversation does not include any application processing overhead. For the paths with serial to Ethernet converter, this offers the least “code start” time period for certain protocols.

Also, frequent TCP re-connections and retransmissions demonstrate an unstable connection, especially for wireless connections.

E. Session, Presentation, and Application Layer
The majority of the functions for Layers 5-7 are logically combined into the “Application Layer” for the purposes of discussion in this paper. Actually, some applications, such as Modbus, DNP3, and IEC 61850 MMS are built immediately upon the Transport Layer. The applications in this layer establish, manage, and terminate application connections, and perform the data conversion, compression, encryption, and decryption.

In this layer, the application misconfiguration or implementation error could cause communication failure.

III. Baselining
After initial setup of the communication, a backup of the configuration of each network component should be retained, and a copy of the normal traffic through the network should be baselined as a successful template. In the rest of this section, we will introduce the necessary hardware, software and the process to create such traffic copies. Also, the tools and the process can be employed to assisting configuring and debugging at the initial setup.

A. Hardware
There are three different types of hardware can be used to sniff the traffic for recording or analyzing, i.e., a hub, a switch with Switch Port Analyzer (SPAN) function (port mirroring), and a network test-access-point (NTAP). NTAPs are recommended for its swift, honest, and non-interfering features. The detailed comparison is listed in Table 1.

B. Software
- Wireshark is employed to capture the traffic with the help of the N-TAPs. The tool can be downloaded from https://www.wireshark.org/ and the basic user guild can be found at https://www.wireshark.org/docs/.
- Some generic windows network diagnose commands will also help understanding the status of the network, including, but not limited to ipconfig, ping, netstat, tracert, pathping, nbtstat, etc.
- Nmap can help scanning the open ports of a given IP to find if a particular service is available, e.g. Modbus port 502, DNP3 ports 20000, and also detect security breaches.

C. Process
To ensure obtaining adequate information, the baselining should be carefully planned.

1) Understand the path of the packets.
For connected switches, with Spanning-Tree Protocol (STP) or Rapid STP (RSTP), the traffic travel through only one of multiple possible paths that connect the source and destination units. So monitoring through other switch ports not on the traffic path won’t catch the intended packets. Finding the correct path is crucial in this case. For the communication with HSR/PRP, the traffic is sent through both LANA and LANB. Therefore, monitoring through both ports are necessary.

### TABLE I. Baseline Hardware Comparison

<table>
<thead>
<tr>
<th>Features</th>
<th>Baseline Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Test Access Point (TAP)</td>
<td>Switch with SPAN (port mirroring) function</td>
</tr>
<tr>
<td>Network Type</td>
<td>10/100/1000 Mbps</td>
</tr>
<tr>
<td>Physical Layer</td>
<td>Copper, Fiber</td>
</tr>
</tbody>
</table>

| Drop Selected* packets   | Yes. Hardware and media errors are dropped. Packets of some selected protocols may be dropped by default settings. E.g. the 1588v2 time request packets will be discarded by certain switches as LLDP packets. Other packets that may be considered as malformed packets, e.g. the oversized PRP packets, etc. |

| Cost                      | Medium - High                                                                    |
| Interference with regular traffic | No interference \ No interference May interfere |
| Need user configuratio n | No Yes. Require professional setup                                              |
| Other Features            | TAPs do not alter the time relationships of frames, spacing and response times VLAN tags are not normally passed through the SPAN port so this can lead to false issues detected and difficulty in finding VLAN issues. |

2) Get the right sniffing/monitoring equipment in the right place.

If possible, an n-TAP should be placed between the monitoring unit and the first switch to obtain a copy of the traffic.

In some cases, to break the communication and insert an n-TAP is impossible either due to the service requirement or security reasons. The SPAN function of the switch can be used instead.

For certain communication structure, VPNs (virtual private networks) are used instead of MPLS for the SCADA to communicate to the remote relay. Since the VPNs employ encrypted and authenticated connections between two hosts, monitoring between two VPN ends is normally futile.

Instead of baselining only from one point, more information can be recorded with simultaneously captures from both the sender’s and the receiver’s end. The monitoring points are commonly selected right in front of the sender and the receiver, as shown in Fig. 2. In this scenario, any issue caused by the network layer or lower, e.g., the corrupted/dropped packets, extremely long delay, unstable connection, packet time sequence inversion, etc., will be easily identified.

3) Compare the baseline to the communication protocols to learn the normal communication pattern.

Observe and get familiar with the normal traffic pattern will help find the communication issue. Validate communication protocol response by comparing the real traffic with the defined behavior. E.g. the TCP 3-way handshake mechanism, the DNP3 IIN bits response, the PTPv2 delay request and response pairs, etc.

Also, comparing the captured packets on both ends of the network will help to locate any missing or corrupted packets that may cause the communication issue. Networks with wireless transceivers or converters (e.g. serial to Ethernet converter) are most susceptible to this kind of distortion.

IV. COMMON TROUBLESHOOTING PROCEDURES

To start troubleshooting, we need to collect as much information as possible to assist finding the proper start point. In Table 2, some typical questions and the corresponding inference are summarized.

A normal work flow of network troubleshooting is suggested below:
<table>
<thead>
<tr>
<th>Questions to Answer</th>
<th>Inference</th>
<th>OSI Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are the applications configured as shown in the communication protocol manual?</td>
<td>Some settings are crucial to ensure the successful communication. Some settings require the match from both the SCADA and relay side. For example, the unit address of the DNP3, the COT of IEC104, etc.</td>
<td>Application Layer</td>
</tr>
<tr>
<td>Will the target unit respond to any TCP protocol, e.g. web service, MMS, Modbus, DNP3?</td>
<td>Validate if other TCP based protocols works and the target unit functions well. If no TCP based communication application can perform correctly, it has a good chance of failure in the transport layer.</td>
<td>Transport (TCP/UDP) Layer</td>
</tr>
<tr>
<td>Does the target unit respond to ping? What is the turn around time?</td>
<td>Validates the target unit can be pinged and record the response time to access the network condition. The target unit may experience connection issues on or below IP layer if the ping statistics for the target unit has a non-zero packet loss rate and an extended round trip time. Due to security concerns, some companies blocks ICMP in their firewall. The ping application relies on the ICMP for notification will fail in this case. The ping command should be customized to address different protocols. For example, for DNP3, the maximum fragment size is 292 bytes, therefore customize the ping command as ping -a -n 100 -l 304 -f [target ip]</td>
<td>Network (IP) Layer</td>
</tr>
<tr>
<td>Is the target unit behind a firewall that blocks the specific port for the specific protocol?</td>
<td>The firewall may block certain communication traffic and cause communication interruption. The Nmap tool can identify the open ports. For example, the web service (HTTP/HTTPS) uses port 80/443, IEC 61850 MMS uses port 102.</td>
<td>Transport (TCP/UDP) Layer</td>
</tr>
<tr>
<td>What’s the network structure? List the brand, model number, firmware version and settings/configuration s of the network equipment on the communication path.</td>
<td>The low layer equipment and protocols have to be compatible and work together to provide a stable data path. Especially, the redundancy settings (HSR/PRP/RSTP), the PTP profiles selection, the serial cable types, etc.</td>
<td>Layer 2 (MAC Layer)</td>
</tr>
<tr>
<td>Which types of data are polling from the target unit and sending across the network? What’s the frequency of the polling?</td>
<td>Access the network traffic for time out/bandwidth consumption. For example, if the polling is too slow, the TCP connection may timeout. The keep-alive messages should be checked. Or, if the data polled is too frequent, it may overwhelm the Ethernet to serial converter</td>
<td>Layer 3 (Network Layer)</td>
</tr>
</tbody>
</table>

1) Compare the running configuration of each network unit with its previous working configuration.

2) Check the physical links are secure and active.

3) Start monitoring the network traffic with n-TAPs and Wireshark, and compare the traffic pattern with the working baseline.

4) For LAN level communication, e.g. GOOSE, make sure the broadcasted message can pass the switch’s filter.

5) For HSR/PRP redundancy communication, both LANA and LANB should carry the same packets, the only difference should be the LANID in the HSR header or PRP trailer.

6) If applicable, apply the TCP packet filter in Wireshark and look for proper SYN and FIN handshakes. TCP three-way handshake mechanism can be used to isolate the communication issue. If no abnormal ended TCP session is observed during the communication failure, the issue is most likely to reside in the application layer. Also look for TCP RST packets and FIN group immediate after SYN group. This is a sign of refused service.

Generally speaking, lower layer error will cause malfunctions in all upper layers. Such as a broken physical connection will mute all communication, a MAC flood will jam all communication, and a TCP open sockets error will cause all web service, DNP3 and MMS not responding. In most cases, an Omni-fail of all protocols on or above a certain layer is a hint of failure in a lower layer, a bottom-up check will save a lot of diagnosing effort.

However, due to the interactive nature of the layers, some errant behavior only happens with certain combinations of the applications from different layers. For example, the PRP protocol will add a 6 bytes Redundancy Control Trailer (RCT) in the Layer 2 (MAC layer). This may cause the MTU incompatibility issue in large file transfer with FTP in the Layer 7 (Application layer), where a single packet’s payload can be 1500 bytes, but won’t cause any issue for DNP3, which has a maximum payload 332 bytes (292 bytes DNP3 + 20 bytes of TCP header + 20 bytes of IP header). This MTU incompatibility error can be detected either with un-echoed ping message in Layer 3 or missing TCP ACK message caught by Wireshark in Layer 4. In this case, a top-down analysis with specially constructed probes will be more effective.

V. SUMMARY

This paper introduced some basic tools and techniques for communication baselining in the SCADA Communication Network (SCN). Also a fundamental process for network analysis and diagnose procedures are introduced. With the development of new communication technologies and protocols, the process should be constantly revisited and update. Furthermore, the process introduced in this paper can also be used for other industrial network scenarios if applicable.