PMU Traffic Scenarios and Network Conditions in IP-Based Wide Area Communication

Jordan Ivanovski
Volkan Maden

A Master Thesis Report written in collaboration with
Department of Industrial Information and Control Systems
Royal Institute of Technology
Stockholm, Sweden

October, 2009
Abstract

The electric power system is a very complicated system to manage and operate due to its size, dynamic nature, fluctuations in demand and the large amount of heterogeneous components and devices. New upcoming technologies such as Phasor Measurement Units (PMUs) offer accurate and timely data on the state of the power system increasing the possibilities to manage the system at a more efficient and responsive level and apply wider monitoring, control and protection schemes.

The communication networks are the foundation for PMU data distribution. The demands on the networks capabilities and data traffic management are rapidly increasing because of new components and data flows. In order to provide efficient data communication and optimal resource usage, it is sufficient to identify and implement mechanisms such as Quality of Service.

In this master thesis, an IP Network has been characterized and modeled. The created models have then been implemented in simulation software, OMNeT++. Several scenarios have been designed derived from the demands and expectations for a wide area communication network. Finally, simulations have been conducted and results regarding End-To-End Latency, Packet Loss and Jitter obtained and analyzed.

Keywords

Quality of Service, PMU, RTU, Wide Area Communication, OMNeT++
Acknowledgments

This work has been carried out as a part of a master thesis project. It is cooperation between the Industrial Information and Control Systems Department at KTH and Svenska Kraftnät.

The authors would like to thank and express their gratitude to Moustafa Chenine, supervisor at KTH as well as representatives from SvK especially Lars Wallin and Henrik Simm for their valuable support throughout this master thesis. Furthermore, we thank our families for their continuous support since the beginning and throughout our studies.

For further information regarding the contents of this technical report please contact the authors (volkan_maden@hotmail.com and jordan_ivanovski@yahoo.com) or the Department of Industrial Information and Control Systems, KTH, Stockholm Sweden.
# Table of Contents

Abstract ................................................................................................................................... 3  
Keywords ................................................................................................................................ 3  
Acknowledgments ................................................................................................................... 4  
1. Introduction ..................................................................................................................... 8  
   1.1 Problem ......................................................................................................................... 8  
   1.2 Aim and Objective ........................................................................................................ 9  
   1.3 Chapter overview .......................................................................................................... 9  
2. Background ....................................................................................................................... 10  
   2.1 Transmission System Operators, TSOs ...................................................................... 10  
   2.2 Wide Area Monitoring and Control, WAMC ............................................................. 11  
   2.3 GridStat ....................................................................................................................... 11  
   2.5 Phasor Measurement Unit (PMU) .............................................................................. 12  
   2.6 Phasor Data Concentrator (PDC) ................................................................................ 12  
   2.7 PMU Data Flow .......................................................................................................... 13  
      2.7.1 PMU Data Characteristics .................................................................................... 13  
   2.8 RTU and SCADA ....................................................................................................... 14  
   2.8 IP Network .................................................................................................................. 14  
   2.9 Quality of Service in IP Networks .............................................................................. 15  
      2.9.1 Resource allocation .............................................................................................. 15  
      2.9.2 Performance Optimization ................................................................................... 17  
   2.10 Network protocols ..................................................................................................... 19  
      2.10.1 UDP .................................................................................................................... 19  
      2.10.2 TCP .................................................................................................................... 19  
   2.11 Data traffic ................................................................................................................ 20  
      2.11.1 Traffic Descriptor ............................................................................................... 20  
      2.11.2 Traffic Profiles ................................................................................................... 21  
      2.11.3 Flow Characteristics ........................................................................................... 21  
   2.12 Requirements ............................................................................................................ 22  
      2.12.1 Applications Requirements ................................................................................ 22  
   2.13 OMNeT++ ................................................................................................................ 23  
3. Methodology ..................................................................................................................... 24  
   3.1 Preparation .................................................................................................................. 25
1. Introduction

The electric power system is a very complicated system to manage and operate due to its size, dynamic nature, fluctuations in demand and the large amount of heterogeneous components and devices involved from the generation of electrical power to the transmission and distribution to the final consumer.

New upcoming technologies such as Phasor Measurement Units (PMUs) offer accurate and timely data on the state of the power system increasing the possibilities to manage the system at a more efficient and responsive level and apply wider monitoring, control and protection schemes.

The communication networks are the foundation for PMU data distribution. The demands on the networks capabilities and data traffic management are rapidly increasing because of new components and data flows. In order to provide efficient data communication and optimal resource usage, it is sufficient to identify and implement mechanisms that can regulate the data traffic in an adequate manner. A suitable mechanism for resource allocation and traffic regulation is a Quality of Service, QoS implementation. In this way different data flows will have reserved capacity on the links and different prioritization levels without affecting or interrupting other data flows. The result of this would be higher reliability and accuracy in delivering data packets especially under heavy network load [1].

1.1 Problem

Along with the growing electricity demands and expanding electric power systems, the demands on a communication network that supports the monitoring and control systems of the power network are increasing. The amount of the existing network traffic continuously increases and new data flows are being integrated in the communication networks, augmenting the overall network traffic. In order to provide secure and reliable data distribution, mechanisms such as QoS have to be implemented in the network. Identification of data flows and requirements establishment is necessary before employing resource allocation and prioritization levels. Figure 1 illustrates the concept of QoS.

![Figure 1 – Network Communication with QoS](image)
1.2 Aim and Objective
The objective of this master thesis is to model network conditions and traffic profiles of a wide area utility network with a focus on PMU data flows. To understand how PMU data flows are affected under different circumstances in a wide area utility network, different scenarios and models are created. These scenarios cover diverse network characteristics, i.e. variation of the network load and usage of different methods to establish appropriate level of QoS. Further on, studying how the presence of both PMU and RTU traffic, along with the IP Telephony and Video traffic, will affect the network functionality and performance. Several simulations are performed in accordance to predefined network scenarios and simulation results are collected. The final objective is to evaluate the obtained results, give recommendations and identify critical factors that improve or degrade the real time streaming of PMU data by studying and verifying the network behavior.

1.3 Chapter overview
This section outlines and presents the structure of this master thesis report.

1. Introduction
The Introduction chapter gives an overview of the power system importance and complexity along with new upcoming technologies such as Phasor Measurement Units, PMUs. Communication networks performance and QoS are introduced as a motive for carrying out this master thesis.

2. Background
Fundamental parts of the electric power system, such as PMUs and PDCs along with their functionalities and specifications are clarified. Furthermore overviews of QoS and IP-network architectures and principles are presented. The simulation tool OMNeT++ is briefly described.

3. Methodology
This chapter gives a chronological view and describes the method which is used for carrying out the master thesis. The methods main and sub phases are described in detail.

4. Implementation
The Implementation chapter presents the created network models and chosen scenarios. It also explains how they have been implemented in OMNeT++.

5. Results and Analysis
The acquired simulation results are presented in this chapter followed by an analysis and evaluation of these results.

6. Discussion
This chapter contains discussions about different issues and thoughts that rose up during the master thesis project. Besides that, certain choices and preferences have been motivated.

7. Conclusions
Finally, recommendations regarding current and future network implementations along with ideas about future work are included in the final chapter.
2. Background

This chapter introduces the reader to the background of this master thesis. Firstly, the role and the responsibilities of Transmission System Operators, TSOs, are being explained and comprised. Further on, Wide Area Monitoring and Control is being described along with Phasor Measuring Units, PMUs and Phasor Data Concentrators, PDCs as the main contributors for the WAMC concept. As reference model for Wide Area Monitoring and Control architecture, GridStat is presented and explained. Wide Area Networks are introduced as foundation for PMU data distribution along with important network protocols. Data flows are then discussed with focus on PMU data flow. Finally, the simulation software used during this master thesis, OMNeT++, is presented.

2.1 Transmission System Operators, TSOs

Transmission System Operators are companies that own national electricity grids and facilitate the power market by making it physically possible to transport power from producers/sellers to buyers. The TSO makes the transport grid available by planning, constructing and operating it in accordance with both political and physical laws. As a state-owned company, the TSO is responsible for the overall physical management and control of the national power system. Svenska Kraftnät, SvK, is the Swedish national TSO and operates and administrates the Swedish national grid which consists of 15 000 km of 220 kV and 400 kV lines [2][3].

![Figure 2 – Electricity Market Overview](image)

The TSO, as the central electricity distribution medium, is the main connection point between the electricity production and the electricity consumption. This makes TSOs position very critical mostly because they are partially responsible for a wide variety of customers receiving electricity.
2.2 Wide Area Monitoring and Control, WAMC
Wide Area Monitoring and Control is a technique that provides real time surveillance of the power grid by collecting measurements from across the grid. A typical WAMC System is built up on a reliable communication system connecting power stations, network control centres and substations. The GPS satellite system is used for timing accuracy and a number of phasor measurement units are deployed across the power network. The phasor measurement unit or PMU streams the required real time data through the communication link to a Phasor Data Concentrator or PDC. In some cases, PMUs could even include local instability protection schemes [4].

There are several grounds that necessitate and facilitate implementation and usage of the WAMC concept. Reliable electricity supply is continually becoming more and more essential for society, and blackouts are becoming more and more costly whenever they occur. Wide-area disturbances have forced/encouraged power companies to design system protection schemes to counteract voltage instability, angular instability, frequency instability, to improve damping properties or for other specific purposes, e.g., to avoid cascaded line trip. Further on, technical developments in communication technology and measurement synchronization, e.g. for reliable voltage phasor measurements, have made the design of system wide protection solutions possible [5].

2.3 GridStat
GridStat is a communication framework designed as a middleware for handling the traffic between PMUs and Control Centre. GridStat is based on a “publish – subscribe” architecture, where the PMUs publish data and applications at the Control Centre subscribe to the data. The GridStat architecture takes advantage of QoS by implementing different layers of QoS brokers which manage the resources on the network and makes sure QoS requirements are met [6]. The GridStat architecture is depicted below in Figure 3.
Even though the examined network is not designed and configured in the same manner as GridStat, it does have similarities. The GridStat architecture thus helps setting parameters and defining requirements for the simulations performed during this master thesis.

2.5 Phasor Measurement Unit (PMU)
The PMU captures measurements of analog voltage, current waveform and the line frequency directly from the grid. After digitizing, the phasor measurements are then stamped with the creation time provided by a GPS clock. Phasor measurement unit transmits samples in different sizes. The PMUs transfer rate can differ and can be between 30 and 60 Hz. 30 Hz involves 30 samples per second while 60 Hz is equivalent to 60 samples per second. When encapsulating its data, the PMU employs the C37.118 protocol [7]. The final PMU packets are transmitted into a wide area network before reaching their destination, the Phasor Data Concentrator PDC. Figure 4 illustrates the structure of a PMU.

![PMU Structure](image)

PMU provides a dynamic system observation of the network, because the measurements are taken with a high sampling rate from geographically distant locations and they are then grouped together according to the time stamp provided by the GPS [8].

2.6 Phasor Data Concentrator (PDC)
A PDC is a device connected to the network which receives data from PMUs. After receiving, it sorts and groups the PMU packets depending on their creation time which involves that PMU packets that arrive at the PDC and have same GPS time stamp are encapsulated in one common packet. These packets are then sent as a stream to appropriate application. Besides that, the PDC also performs a number of quality checks, such as inserting appropriate flag in the correlation of data, checking for disturbance flags and recording the data for offline analysis [9].

Depending on the network architecture and size, some PDCs may act as Super PDCs. These PDCs collect information both from PMUs and other PDCs and are often connected to a central database for long-term archiving of the data [10].
2.7 PMU Data Flow
The main data flow which is of importance for this master thesis is the PMU to Control Centre data flow. The process starts with the PMU reads sensor data from the power grid. After converting the analog signal into digital via an AC/DC Converter built in the PMU, the data combined with the GPS time stamp is encapsulated into packets. These packets are then forwarded to the PDC via the WAN, where the packet passes through several routers. The original packet size is intact due to routers not modifying the packet size.

When the packet has arrived at the PDC, it has been buffered, synchronized and grouped into larger PDC packet consisting of data from multiple PMU packets. The packets, after being processed in proper applications in the Control Centre, are stored in databases with different purposes [6][10]. At this point it is important to notify that the other identified data flows are considered as background traffic and estimated along with SvKs experts. Figure 5 depicts the PMU data flow:

![Figure 5 – PMU Data Flow](image)

2.7.1 PMU Data Characteristics
PMU data is synchronized by a timestamp from a GPS. According to the C37.118 standard, a PMU message frame should be represented with the frame format illustrated below.

<table>
<thead>
<tr>
<th>First transmitted</th>
<th>LAST transmitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYNC (2 bytes)</td>
<td>FRASESIZE (2 bytes)</td>
</tr>
<tr>
<td>IDCODE (2 bytes)</td>
<td>SOC (4 bytes)</td>
</tr>
<tr>
<td>SOC (4 bytes)</td>
<td>FRACSEC (4 bytes)</td>
</tr>
<tr>
<td>DATA 1</td>
<td>DATA 2</td>
</tr>
</tbody>
</table>

A data frame consists of several parts as illustrated below.

| STAT (2 bytes) | PHASORS (4/8 bytes) | FREQ (2/4 bytes) | DFREQ (2/4 bytes) | ANALOG (2/4 bytes) | DIGITAL (2 bytes) |
According to the standard, a simple PMU frame will consist of 16 bytes. Including a data frame will add 24 bytes to the already existing 16 bytes and result in a total of 80 bytes. Depending on different configurations of the PMU, the amount of data frames and the size of each data frame will vary [11]. For further information about the contents of the frames, the reader is advised to look at the standard C37.118.

2.8 RTU and SCADA
Remote Terminal Units, RTUs, are a part of a SCADA system. These systems are used in various areas, anything from monitoring the state of environmental conditions in buildings to monitoring activity in nuclear power plants [12].

The relevance of RTUs in this master thesis is that they are used to provide real time data concerning the current state of a power grid and also perform control actions on the power grid. The information gathering is done by measuring analogue and digital signals from sensors, and sending this information to an application situated in the Control Centre [13].

The importance that RTUs impose in this master thesis is the traffic they generate in the network. An essential aspect for investigation is how RTUs and PMUs can use the same network to send their data through. An outcome of this analysis provides knowledge about how the network is able to handle the extra traffic imposed by the added RTUs and how this affects the PMU traffic.

2.8 IP Network
The backbone of the examined IP network is built of fiber optical cables that are used as a transmission medium. These cables connect different parts of the network and by doing so also enabling communication between those parts. Building up the network simply with cables is not sufficient. In order to regulate and prioritize the transmitted information, the IP network contains several connection points in form of access and core routers [14].

Without prioritization schemes and traffic regulation, this kind of data exchange is not optimal in terms of latency and packet loss. This is the reason why the core routers exist at the connection points. They have the capability of regulating the traffic and reserving bandwidth for different data flows. The routers operate on IP-level, therefore, they know which route is most appropriate to send information on. By regulating the traffic on the links, the chances of congestion decrease thus also decreasing the latency and packet loss. Besides the core routers, the network contains access routers that different kinds of equipment such as PMUs, Video and IP-telephones are connected to. The main task of an access router is to set different prioritization schemes for different data flows and then send the traffic into the core network. Each access router has double 2Mbit/s channels enabling redundancy on the network. To separate the different data flows on the network, SvK has chosen to have separate VLANs for the different data flows. IP-telephony has its own VLAN, as well as internet connection. This results in different IP-address domains for the different kinds of traffic [14]. Figure 6 presents a simplified model over the IP network.
Figure 6 – IP Network Overview

2.9 Quality of Service in IP Networks

Quality of Service is often referred to the capability of providing resource assurance and service differentiation in a network.

In order to enable QoS and address some of the fundamental issues in the Internet, such as resource allocation and performance optimization, several techniques and mechanisms have been developed in the recent years. Some of them are the following: Integrated Services, Differentiated Services, Multiprotocol Label Switching (MPLS) as well as Traffic Engineering.

Integrated Services and Differentiated Services are two resource allocation techniques for the Internet that enable resource assurances and service differentiation for traffic flows and users. On the other hand, MPLS and Traffic Engineering provide management tools for bandwidth provisioning and performance optimization which are fundamental in supporting QoS on a large scale and at a rational cost [1][15].

2.9.1 Resource allocation

Resource allocation is associated with network issues such as dropping packets and packet latency. These issues arise when the network resources cannot fulfill the traffic demands. IP networks with their heterogeneous structure include shared resources such as bandwidth and buffers which have to be divided and planned appropriately.

Even though, the Internet today provides a best-effort service with no real resource allocation opportunity and the Transmission Control Protocol (TCP) as a congestion avoidance and detection tool, two new resource allocation techniques have been developed,
Integrated Services and Differentiated Services. These techniques provide some important concepts for the networks QoS support [1]:

- Frameworks for resource allocation that support resource assurance and service differentiation
- New service models for the Internet in addition to the existing best-effort service
- Language for describing resource assurance and resource requirements
- Mechanisms for enforcing resource allocation

**Integrated Services**
The Integrated Services technique is based on per-flow resource reservation which means that before being able to transmit data over the network an application has to obtain appropriate resource assurance by making a resource reservation. The resource reservation involves the following steps [1]:

- The application characterizes its traffic source and the resource requirements.
- Based on the requested resources the network finds a suitable path for the data flow by using a routing protocol.
- The reservation state is being installed alongside the established path where at each hop admission control is used to verify whether adequate resources are available before accepting the new reservation.
- The reservation is established.
- The application can start transmitting data over the path.

During the data transmission, the application has exclusive use of the resources in the established path where resource reservation is enforced by packet classification and scheduling mechanisms in the network routers.

There are two service models that can be chosen: the guaranteed service and the controlled load service model. The guaranteed service model, by using firm admission control and fair queuing scheduling, ensures deterministic maximum delay and it is associated with applications that demand strict delay limitations. On the other hand, the controlled load service model provides less strict guarantees and is closely related to a lightly loaded best-effort network.

The Integrated Services technique is suitable for resource reservation and allocation in corporate networks operated by a single administrative domain. It can support and provide guaranteed bandwidth for IP-telephony and video conferencing for instance. Resource reservation and allocation for traffic going to a WAN can be accomplished by using the *Resource Reservation Protocol* (RSVP).

**Resource Reservation Protocol (RSVP)**
RSVP is an Internet control protocol used to allocate resources for data flows in a network. Although RSVP may seem like a routing protocol, it is not. It works together with routing protocols to maximize the performance of a network. This is done by enabling hosts in the network to use RSVP for requesting data flow resources. Because of the fact that RSVP is
receiver oriented, the receiving host must initiate and maintain the resource reservation for its data flows. A request for resources typically results in reserved resources in every node along the data route [1][15]. Figure 7 illustrates the implementation and functionality of RSVP.

Figure 7 – RSVP Overview

- **Differentiated Services**
  Differently from the Integrated Services, where per-flow reservations are made, the Differentiated Services technique uses edge policing, provisioning and traffic prioritization in order to accomplish service differentiation.

Differentiated Services do not demand resource reservation. The traffic is divided into forwarding classes where the amount of data that users can transmit is regulated and limited at the networks periphery. The aim with this is that service providers can control the resource assurance to the users and thereby the amount of traffic in the network.

Packets are being mapped to adequate forwarding classes based on *Service Level Agreement* (SLA) between the users and their service provider. The forwarding classes are embedded in the packets headers and are being used by the networks internal nodes for distinguishing the treatment of the packets, drop priority or resource priority.

Differentiated Services technique is suitable for transaction-oriented web applications [1][15].

2.9.2 Performance Optimization
Performance Optimization is associated with efficient network resource organization aiming to maximization of the probability for data delivery and minimization of the cost of the same.

It is well known that in the present Internet when paths are being established the shortest-path algorithm is used which often results high rejection rate and poor utilization. Not using diverse network connections and the presence of congestion causing bottlenecks leads to uneven traffic distribution in the network [1].
Two mechanisms that can be used in order to tackle these issues are: *Multiprotocol Label Switching* (MPLS) and *Traffic Engineering*.

- **Multiprotocol Label Switching (MPLS)**
  When a packet traverses across a network it makes hops and passes through different nodes. Choosing the next hop is done by dividing incoming packets into a set of *Forwarding Equivalence Classes* (FECs) and mapping FECs to a next hop. In conventional IP forwarding the packets header is being examined at each hop and assigned to a FEC. With MPLS, on the other hand, the packet to FEC assignment is done only before the first hop when the packet enters the network. The FEC that the particular packet is assigned to is embedded in form of a short fixed value called label which is attached to the packet before being forwarded. The packet forwarding is done by examining the packets current label and after identifying the next hop replacing it with a new label for the next hop. No header analysis is needed at the internal network nodes [1][15]. *Figure 8* illustrates the implementation and functionality of MPLS.

![Figure 8 – MPLS Overview](image)

- **Traffic Engineering**
  When using conventional destination-based IP routing, it is difficult to accomplish balanced traffic distribution in a network which is the key for resource optimization and congestion minimization. In Traffic Engineering, an advanced route selection technique known as constraint-based routing is used in order to achieve these aims. Traffic trunks are calculated based on network-wide information on topology and traffic demands. A traffic trunk is an aggregation of traffic flows associated with the same class, included in a so called *Layered Service Provider* (LSP). The traffic belonging to a specific trunk has the same label and class of service field in the MPLS header. Traffic trunks do not borrow bandwidth from neighbouring trunks neither do they lend unused bandwidth to other trunks which results in evenly distributed bandwidth.
Constraint-based routing uses traffic demands between edge nodes when selecting sets of routes for the logical connections. After the routes have been computed, MPLS can be used to establish logical connections as LSPs.

The disadvantage of constraint-based routing is revealed when a network grows in number of edge nodes which implies growing number of logical connections established. This results in growth in messaging overheads and risk for breakdown of multiple logical links in case of a link breakdown.

An alternative way for achieving the desired traffic distribution is by manipulating link weights and using the *Open Shortest Path First* (OSPF) routing protocol. This is a more cost-effective solution since it does not require extensive changes in the network architecture.

### 2.10 Network protocols

There are several protocols used for data transportation in communication networks. A trivial description of the *User Datagram Protocol* (UDP) and *Transmission Control Protocol* (TCP) is presented below.

#### 2.10.1 UDP

The User Datagram Protocol is a protocol used for transmitting data from a sender to a receiver. UDP is a connectionless protocol which means that a connection between two hosts is not set up before data is sent. In this case, the sender will not know if a packet has reached its destination or not and continue sending until there all data is sent. Easily explained, UDP relies on the networks ability to transfer the data from the sender to the receiver, which might result in some data being lost. The positive side with UDP is the ability of high-speed data transmission. As a conclusion, UDP is usually used by applications that need fast performance, i.e. Video or IP-Telephony [16].

#### 2.10.2 TCP

The Transmission Control Protocol is nowadays often described by the OSI reference model while in the 1970s it was initially described by the TCP/IP reference model. TCP, among other similar protocols, is used to transfer data in networks or network of networks. Compared to UDP, it is a more reliable protocol due to more functionality. TCP is a connection oriented protocol; it requires a connection to be established between two hosts in order to transfer data through a network. When a connection is established, it is kept until the data is sent or the connection is timed-out. As data is prepared for sending using TCP, it is split up in smaller parts called segments which are sent and hopefully received. To assure complete transfer of data, hosts using TCP send acknowledgments when they receive a segment. This way, the sender will know that the receiver received the sent segment. A sending host has timers for segments. When an acknowledgment is not received and the segment is timed-out, the receiver will send the segment again and by doing so assuring reliability. As a consequence to the added functionality, TCP is slower than UDP which might not be a wished quality in cases as Video- or IP-Telephony traffic [16].
2.11 Data traffic
Data traffic is one of the main issues that QoS directs at. Quality of Service can be seen as establishment of appropriate environment for the data traffic circulating in the network [17].

2.11.1 Traffic Descriptor
Data flows can be represented with help of qualitative values even called traffic descriptors. *Figure 9* illustrates an example for a traffic descriptor:

- **Average Data Rate**
The average data rate is the correlation between the number of bits sent during a period of time and the number of seconds in the period. It is a very useful traffic characteristic because it specifies the traffic requirements for average bandwidth needed. The following formula presents this correlation:

\[
Average \ data \ rate = \frac{Amount \ of \ data}{Time}
\]

- **Peak Data Rate**
Peak data rate defines the maximum data rate a specific traffic can have. It specifies the potential maximum bandwidth the traffic can require.

- **Maximum Burst Size**
Maximum burst size defines the longest time period that a specific traffic can flow with its peak data rate.

- **Effective Bandwidth**
The bandwidth that the network needs to allocate for a specific data flow or traffic is also known as effective bandwidth. It presents a correlation between the average data rate, peak data rate and maximum burst size.
2.11.2 Traffic Profiles
There are three different traffic profiles a data flow can have, constant bit rate, variable bit rate and bursty bit rate. The PMU data flow has a constant bit rate profile and it’s illustrated in Figure 10:

![Figure 10 – Traffic Profile for PMU Data Flow](image)

2.11.3 Flow Characteristics
There are four different characteristics that are attributed to a data flow, reliability, delay, jitter and bandwidth [17]. Figure 11 illustrates this correlation:

![Figure 11 – Flow Characteristics](image)

- **Reliability**
Reliability is a flow characteristic associated with the application requirements regarding reliable data transmission. Lack of reliability implies packet and or acknowledgment loss which leads to data retransmission. Different applications have dissimilar reliability requirements.

- **Delay**
This is another flow characteristic which is regulated and adjusted depending on the applications requirements and delay tolerance.

- **Jitter**
Jitter is a flow characteristic that represents how big the variation in packet delay is, constant or variable. Certain applications demand low and/or constant jitter while other applications can tolerate higher and/or variable jitter.

- **Bandwidth**
Bandwidth defines the applications demands and needs for link capacity.
2.12 Requirements
There are several different applications that employ and process PMU data operating at the control centre site. Most frequently used applications are Voltage Instability Assessment application, Frequency Instability Assessment application and Oscillation Monitoring and Control application [18]. Regarding the PMU data delivery, each of the applications has specific requirements that have to be fulfilled. The requirements for respective application are presented below. Further requirements relating to real time wide-area monitoring and analysis such as Phasor Data requirements, Data Delivery requirements and PDC requirements [19][20] are presented in Appendix A.

2.12.1 Applications Requirements

- **Voltage Instability Assessment**

  Table 1 – Voltage Instability Assessment Requirements

<table>
<thead>
<tr>
<th>Interviewees</th>
<th>SvK</th>
<th>NASPI*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expected Latency</td>
<td>1 to 2 seconds (Long term)</td>
<td>Few seconds</td>
</tr>
<tr>
<td>Expected Resolution</td>
<td>Low</td>
<td>30 Hz</td>
</tr>
<tr>
<td>Expected Time Window for Response</td>
<td>Less than 1 minute</td>
<td>Min/Sec for Long/Short term voltage stability</td>
</tr>
<tr>
<td>Format/ Protocol</td>
<td>C37.118</td>
<td>C37.118</td>
</tr>
<tr>
<td>Time Delay for Current/Tested Control Schema</td>
<td>From 200-300 ms to 1 s (on a dedicated channel)</td>
<td>N/A</td>
</tr>
</tbody>
</table>

*North American SynchroPhasor Initiative

- **Frequency Instability Assessment**

  Table 2 – Frequency Instability Assessment Requirements

<table>
<thead>
<tr>
<th>Interviewees</th>
<th>SvK</th>
<th>NASPI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expected Latency</td>
<td>0.25-0.5 seconds</td>
<td>1-5 seconds</td>
</tr>
<tr>
<td>Expected Resolution</td>
<td>50 Hz</td>
<td>30 Hz</td>
</tr>
<tr>
<td>Expected Time Window for Response</td>
<td>0.15 seconds</td>
<td>Few minutes</td>
</tr>
<tr>
<td>Format/ Protocol</td>
<td>C37.118</td>
<td>PDC Stream/C37.118</td>
</tr>
<tr>
<td>Time Delay for Current/Tested Control Schema</td>
<td>Not Applicable</td>
<td>N/A</td>
</tr>
</tbody>
</table>
• Oscillation Monitoring and Control

Table 3 – Oscillation Monitoring and Control Requirements

<table>
<thead>
<tr>
<th>Interviewees</th>
<th>SvK</th>
<th>NASPI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expected Latency</td>
<td>0.25-2 or 3 seconds</td>
<td>1-5 seconds</td>
</tr>
<tr>
<td>Expected Resolution</td>
<td>10/50 Hz for online/offline applications</td>
<td>10 Hz</td>
</tr>
<tr>
<td>Expected Time Window for Response</td>
<td>N/a</td>
<td>Seconds</td>
</tr>
<tr>
<td>Format/ Protocol</td>
<td>C37.118</td>
<td>PDC Stream/C37.118</td>
</tr>
<tr>
<td>Time Delay for Current/Tested Control Schema</td>
<td>0.25 seconds</td>
<td>N/A</td>
</tr>
</tbody>
</table>

2.13 OMNeT++

OMNeT++ is a component-based simulation environment which supports GUI. It is used for simulating communication networks and collecting specific data from those simulations. OMNeT++ is rapidly becoming a popular simulation platform in the scientific community, which is why the students have chosen to use it. Numerous open source simulation models have been published, in the field of internet simulations (IP, IPv6, MPLS, etc), mobility and ad-hoc simulations and other areas.

The INET/MANET framework is an add-on to OMNeT++. The framework provides ability for implementation of advanced network protocols such as RSVP and MPLS. These protocols, among other, are represented as simple components and the functionality aspects of these types of components are programmed in C++. Larger components, for instance routers which can handle advanced protocols are built up by combining and connecting several simple components together [21].

The OMNeT++ environment allows simple execution of simulations. The existence of different simulation modes enables the user to choose among different simulation modes, i.e. step-by-step, fast, and express.
3. Methodology

During this master thesis a case study has been carried out. Case studies are often performed as field studies performed at organizations or companies. Both students have previous experience and are well familiar with the method. The following definition describes the method:

“An empirical study that examines a contemporary phenomenon in its real context, especially when the border between the phenomenon and the context is unclear. The study is based on several sources, where data collection and analysis are guided by theoretical assumptions.” [22].

There are six fundamental phases that have been conducted simultaneously, Preparation, Network modeling, Implementation, Simulation, Evaluation and Summarization. Figure 12 is an illustration of the method, pointing out the main and the sub phases being a part of the method.

![Figure 12 – Method Overview](image-url)
3.1 Preparation
The first step in the method implementation is the Preparation phase. It consists of two sub phases, Literature study and Investigation of the network architecture. It constitutes a very important part of the method because it is the basis for the project and the biggest factor which the final result and the outcome of the project depend on.

- **Literature study**
  For carrying out the master thesis successfully, there were several important issues that the students had to get familiar with, such as QoS in a network context, Network Design, Real time data flow and transport, Wide Area Monitoring and Control (WAMC), Synchronized Measurement Technology (SMT), PMUs, PDCs. In order to understand these issues and build up a reliable and valid data base which was used as a main reference while carrying out the project, relevant literature in form of books, manuals and e-articles were carefully gathered in coordination with the master thesis supervisor.

- **Investigation of the network architecture**
  Furthermore, in order to achieve as realistic and relevant results as possible which SvK could benefit from, the investigation of the network architecture was of crucial importance. The students gathered applicable information and facts about the examined WAN and thus became competent and knowledgeable enough to use that information later on when modeling the network. This was achieved by interviewing relevant employees and experts at SvK, gathering documents such as technical specification of hardware/software as well as documentation from previous researches conducted at SvK.

3.2 Network modeling
The second step of the method implementation is the Network modeling phase which consists of two sub phases, Creation of traffic models and Creation of network models.

- **Creation of traffic models**
  In this sub phase the ambition was to identify and specify the different traffic flows, apart from the PMU flow, traversing the network. These separate traffic flows together are representing the background traffic in the network. Defining them in an accurate manner is essential for creating appropriate network simulation environment which increases the validity and the transparency of the results obtained in this master thesis. Modeling these traffic flows involved definition of several parameters such as data rate, packet size, protocol headers etc.

- **Creation of network models**
  After defining and modeling the traffic flows, network models were created that correspond to the examined network. The models were based on network information such as amount of units, hosts, routers, links etc. Regarding the inability of integrating all the units, that are part of the real network, certain scaling was needed when creating the network models. This implies defining correlations between the model hosts and
the real network hosts where for instance one model host is equivalent to several real network hosts. The network models were designed in a correspondence with the predefined network scenarios.

3.3 Implementation
The third step of the method implementation is the Implementation phase which consists of two sub phases, Implementation of the models in OMNeT++ and Metrics selection.

- **Implementation of the models in OMNeT++**
  As a preparation for this sub phase, studying of OMNeTs infrastructure and functionality was required in order to implement the created models in a correct manner. The implementing of the models was carried out gradually, starting with a simpler models consisting of only few network units and integrating additional units into the network until the final network architecture was obtained. The functionality of the models was verified by simulating the network and examining the resulting outputs.

- **Metrics selection**
  Metrics selection was performed in accordance to literature studies and OMNeTs measuring possibilities. The following metrics were chosen for investigation of the QoS fullness and performance of the network:
  - **End-to-End Latency**
    End-to-End Latency refers to the time taken for a packet to be transmitted across a network from source to destination. It is a summation between the packets transmission, propagation and processing delay.
  - **Packet loss**
    Packet Loss is a measurement which indicates the amount of packets dropped in the network. Depending on data flow requirements as well as criticality, the acceptance for packet loss values varies.
  - **Jitter**
    Jitter is difference of data latency. It is mainly measured at the destination and it points out how stable a network configuration is. If jitter is high, it can affect the performance of time-sensitive applications which needs a continuous stream of data.

3.4 Simulation
The fourth step of the method implementation is the Simulation phase which consists of two sub phases, Simulating different scenarios in OMNeT++ and Gathering network simulation results.

- **Simulating different scenarios in OMNeT++**
  When all the network models were successfully integrated in OMNeT++ the simulation phase could be carried out. The simulations were performed beginning with the first scenario, where the network was simulated under normal and heavy load respectively.
In the same manner the simulations of scenario two and three were consecutively carried out.

- **Gathering network simulation results**
  When the simulations were carried out, the storage of the traffic information was done simultaneously by accumulating network traffic data in the OMNeT++ specific vector and scalar files. After every performed simulation, different graphs were obtained in accordance with the previously chosen metrics and saved in separate files.

### 3.5 Evaluation
The *Evaluation* phase consists of two sub phases, *Evaluation of the network simulations* and *Result Analysis*. As presented in the *Method model, Figure 12*, the evaluation process along with the literature study phase has iterative characteristics. This implies that during the evaluation phase consultation with the gathered literature is required in order to verify the achieved simulation results.

- **Evaluation of the network simulations**
  Evaluation of the network simulations encompasses different network scenarios and as a result it gave the students valuable information of how different network configurations can impact network behavioral characteristics.

- **Result analysis**
  During this sub phase the acquired measurements were observed and analyzed resulting in concrete results and values for the different metrics.

### 3.6 Summarization
Final phase of the method is the *Summarization* phase of the master thesis with two sub phases, *Revision* and *Presentation*.

- **Revision**
  During this sub phase, the conducted work is revised and altered where required. This is done in collaboration with the involved parties, namely KTH and SvK.

- **Presentation**
  In the last sub phase, the master thesis is orderly documented and presented at KTH and SvK.
4. Implementation

In this chapter the network model used during the simulations is presented and clarified along with description about the OMNeT++ implementation. The model was built and designed in accordance with information acquired from interviews with SvKs experts and previous surveys, master thesis and case studies carried out at Svenska Kraftnät. Information regarding different parameters used during the simulations, such as packet size and data rate, was initially gathered from several literature sources correlated with NASPI, North American SynchroPhasor Initiative, architectures and standards which was evaluated and confirmed later by SvK. Network topologies and protocols were obtained strictly from the interviews and the available survey, the master thesis and case studies [9][14]. At this point it is essential to identify and distinguish the different data flows circulating in the network and get familiar with their characteristics as well as their network capacity requirements and occupation. In this project, work the PMU related data flows have the greatest importance. Apart from the PMU data flow, there are three other data flows that have been taken into consideration, namely RTU-, Video- and IP Telephony-data flows [23]. The models used during this master thesis represent an approximation of the communication network used by Svenska Kraftnät, SvK. The outcome of this study is nevertheless utilizable for other Transmission System Operators.

4.1 Network Model

*Figure 13* presents a geographical interpretation of the network model which is used during the simulations. The network is build upon three types of main nodes, Control Centre, Core Network and Subnet, all illustrated and described in the subchapters 4.1.1, 4.1.2 and 4.1.3 respectively. The Control Centre is located in Stockholm and is connected to a Core Network which is part of the WAN. Further on, there are five subnets situated on different locations across Sweden and are connected to the Core Network.

*Figure 13 – Geographical Network Model*
4.1.1 Control Centre

*Figure 14* illustrates a closer look at the architecture and devices in interest which are part of the Control Centre, situated in Stockholm. The most fundamental device is the Phasor Data Concentrator, PDC, which receives data packets from the PMUs. After receiving, it sorts and sends the packets as a stream to appropriate applications. Data packets generated by video surveillance are directed to the Control Centre’s Server, SRV. An Eth 100Mbit line connects both the PDC and the SRV to a 3Com 5232 Access Router (E2 2Mbit*2), LSR10 in the figure, which in turn is connected to the Core Network with E3 34Mbit optical lines.

![Figure 14 – Control Centre Overview](image)

4.1.2 Core Network

The topology of the Core Network is illustrated in *Figure 15*. A Hybrid Meshed topology is used with 3Com 5632 Core Routers (channelized E3 interface), LSR2, LSR4, LSR5 and LSR6 in the figure, connected to each other with E3 34Mbit optical lines. The Core routers are in turn connected to the subnets access routers with E1 2Mbit line. Two of the core routers, LSR5 and LSR6, are connected to the Control Centre with E3 34Mbit optical lines.

![Figure 15 – Core Network Overview](image)
4.1.3 Subnet

*Figure 16* illustrates the architecture and devices which are part of the Subnet_1. There are five subnets situated across Sweden each of them consisting of two data generators in form of PMU and Video. In order to clarify, the Video device generates the data traffic coming from the camera surveillance which is distributed to the Control Centre Server while the PMU data is distributed to the PDC. The video devices are controlled from the control centre and are only used when desired. This results in video traffic circulating the network periodically. Both devices are connected to a 3Com 5232 Access Router (E2 2Mbit*2), LSR1 in the figure, with Eth 100Mbit lines. Further on, the substation access routers are connected to a regional Core Router with an E1 2Mbit line.

![Figure 16 – Subnet 1 Overview](image)

4.2 Network scenarios

In order to examine and evaluate the network behavior under different circumstances and conditions and be able to identify the most suitable and efficient network configuration, two main scenarios have been chosen. Additional two scenarios, *Scenario 3* and *Scenario 4*, have been chosen intended to present a future implementation of eight additional PMUs in the network, sixteen in total, along with IP Telephony traffic. Moreover, in *Scenario 4*, the RTU data traffic has been taken into consideration and included in the network.

The first scenario covers the PMU communication along with the background traffic in the network without QoS schemes. *Scenario 1*, *2* and *3* involve implementing different QoS schemes which means that QoS is applied to all data traversing the network. Furthermore, in the first two scenarios, two distinct scenarios have been implemented, simulating the network traffic under normal and heavy load respectively. This was achieved by simulating the networks without and with video traffic.

Regarding the router traffic it is established that the routing protocol used in the network is OSPF and two major types of router data have been acknowledged as listed below [24].

- Link state packets (Information about the network)
- Hello packets (Neighbor discovery in the network)
These packets are taken into consideration during the simulations by using the OMNeT++ implementation of OSPF in all scenarios.

When implementing the network model in OMNeT++, Point to Point connections are used for connecting the different nodes since each message packet has only one possible receiver, either the PDC or the Control Center Server. According to the C37.118 protocol standards, the PMU packet is 40 Bytes long taken in hand that the packet consists of one Phasor measurement [11]. Table 4 summarizes data rates, payloads, reserved link capacity and different protocol header sizes for each of the data flows used during the simulations.

<table>
<thead>
<tr>
<th>Data flow</th>
<th>Data Rate</th>
<th>Payload</th>
<th>Reserved Link Capacity*</th>
<th>Headers</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMU</td>
<td>30 packets/sec</td>
<td>40 bytes</td>
<td>2240 bytes</td>
<td>UDP/IP</td>
</tr>
<tr>
<td>RTU</td>
<td>2 packets/sec</td>
<td>500 bytes</td>
<td>1100 bytes</td>
<td>28 bytes</td>
</tr>
<tr>
<td>Video</td>
<td>200 packets/sec</td>
<td>1024 bytes</td>
<td>250000 bytes</td>
<td>28 bytes</td>
</tr>
<tr>
<td>IP Telephony</td>
<td>62 packets/sec</td>
<td>1024 bytes</td>
<td>90000 bytes</td>
<td>28 bytes</td>
</tr>
</tbody>
</table>

* Reserved link capacity intended for RSVP in Scenario 2, 3 and 4
** Intended for Super RTUs

Since RSVP and MPLS provide high reliability and accuracy in data delivery, the UDP/IP is used as a transport protocol for all the data flows, including the PMU data flow, in all scenarios. The choice of UDP is further motivated in the chapter 5.7 TCP and UDP.

### 4.2.1 Scenario 1.a and 1.b

In order to examine the PMU data flow behavior under normal and heavy network load respectively, Scenario 1 has been divided into two separate parts, 1.a and 1.b. In the first case, only the PMU traffic is present in the network, whereas in the second case the video traffic has been included by enabling two video hosts to generate and send traffic into the network. The video traffic is configured so the corresponding packets are sent to the Control Centre server, SRV.

These network scenarios demonstrate a network environment where eight PMUs are integrated in the network along with five video hosts. QoS schemes are not applied to the different data flows. It means that the data packets are treated with the same priority and they all share the available link capacity. Thus, the data delivery in the network is in best-effort manner.
The PMU data has high priority and criticality which implies that high packet loss is not acceptable. This is why the UDP protocol might not be the best choice in Scenario 1, but is used to acknowledge the differences and effects which are contributed by using QoS schemes. Video represents the background traffic in the network. Because of lower criticality and priority, UDP is also used as a transport protocol for data packets belonging to the Video data flow. These scenarios are illustrated in Figure 17.

4.2.2 Scenario 2.a and 2.b
Similarly to the previous scenario, Scenario 2 has been divided into two separate parts, 2.a and 2.b. In the first case, the PMU data represents the total amount of network traffic, while in Scenario 2.b the video traffic has been included by enabling the same video hosts as in Scenario 1.b. This was done in order to achieve the same network conditions as in Scenario 1.b, thus enabling an easy comparison between the two scenario results. The video traffic is again configured so the corresponding packets are sent to the Control Centre server, SRV.

These scenarios demonstrate a network environment where QoS schemes are applied to all data packets circulating in the network. This means that the different data flows have reserved capacity on the links, depending on respective requirements and data rate peak values, without affecting or interrupting the other flows. In order to achieve this, the RSVP and the MPLS protocols have been implemented. Similarly to the previous scenarios, there are eight PMUs in the network and five video hosts. Figure 18 illustrates Scenario 2.a and 2.b.
In this network configuration, RSVP-TE capable routers are used. RSVP occupies the Transport Layer; however, it is not a transport protocol itself. RSVP uses transport protocols to route packets. For accurate routing and packet delivery it is essential to establish a unique ID for each separate data flow. This enables the RSVP routers to distinguish between different incoming packets and route them into an appropriate path. UDP has been used as a transport protocol for all data flows.

4.2.3 Scenario 3
The objective with Scenario 3 and Scenario 4, described in the next section, is to investigate the capability and capacity of the core network to handle and distribute an increased amount of data traffic. In order to achieve enhanced network traffic, additional eight PMUs have been added to the network. Further on, IP Telephony traffic has been integrated in the network in form of three different hosts, IP_Tel_1, IP_Tel_2 and IP_Tel_3. The IP Telephony hosts are directly connected to either a core router or an access router and send their packets to the Control Centre Server, SRV, along with the video traffic. The upgraded network used in this scenario is displayed in Figure 19.

![Figure 19 – Scenario 3](image)

Similar to the previous scenario, RSVP and MPLS are implemented to all three data flows present in the network. UDP is used as a transport protocol. The PMU data flow in particular acquires the same amount of reserved bandwidth in the network as in Scenario 2.
4.2.4 Scenario 4

Finally, Scenario 4 conveys additionally increased network traffic by integrating RTU traffic in the current network. Traffic management and regulation is once again achieved by implementing RSVP and MPLS to the different data flows. The scenario is illustrated in Figure 20.

Concerning the RTU traffic it has been decided, together with SvKs experts, that approximately 200 RTUs shall be integrated into the network and send data to the control centre. Instead of adding 200 real RTU hosts in the network, 10 super RTU hosts have been integrated where each super RTU_X_Y corresponds to twenty real RTUs by increasing the RTU data transmission rate to 40 packets/sec.

The outcome and the results obtained in scenarios 3 and 4 indicate possible necessary upgrades in the network for it to function in an acceptable manner. Full size overviews of the networks used in the different scenarios, implemented in OMNeT++, are presented in Appendix B.

Table 5 presents the differences and correspondences between the different scenarios.

<table>
<thead>
<tr>
<th>Scenario/Property</th>
<th>QoS</th>
<th>PMUs</th>
<th>RTUs</th>
<th>IP Tel.</th>
<th>PMU Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scenario 1</td>
<td>No</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Scenario 2</td>
<td>Yes</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Scenario 3</td>
<td>Yes</td>
<td>16</td>
<td>0</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Scenario 4</td>
<td>Yes</td>
<td>16</td>
<td>200</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

All the simulations have been performed with the same time length of 25 minutes. The four different flows in the network have constant data rates and packet sizes, which implies that there are no deviations in the amount of traffic circulating the network.
4.3 Metrics Measurement Methods
The important aspect with different metrics is the quality they bring when analyzing and inspecting the validity of results. Different methods for metrics measurement have been chosen and implemented. These methods are described below. The measuring is performed at the PDC, located at the Control Centre, and it implies that the graphs are based on results for all incoming PMU packets from different PMUs.

4.3.1 Jitter Measurement
Due to the simplicity and the accuracy of the formula below,

\[ \text{jitter}_n = |\text{Latency}_n - \text{Latency}_{n-1}| \]

it has been chosen as the jitter measurement method. The formula measures the difference in the latency between the currently handled packet and the previous packet [25]. This value is then stored in a vector together with a time value in order to enable a graphical representation of the measured jitter values.

4.3.2 End-to-End Latency Measurement
The End-to-End latency of a certain data flow is measured by calculating the time it takes for every packet to reach its destination. This calculation is done by following the formula stated below:

\[ \text{Latency}_n = \text{Arrival time}_n - \text{Sending time}_n \]

The formula takes advantage of the timing possibilities in OMNeT++. By subtracting the packet sending time from its arrival time, the packet latency is obtained.

4.3.3 Packet Loss Measurement
The packet loss measuring is performed by subtracting the total amount of sent PMU packets by the amount of received PMU packets at the PDC. However, there is an issue that arises when carrying out the simulations, namely the PMU packets that haven’t reached the PDC at the moment when simulation ends and are thereby still in the network cannot be considered neither as lost or arrived. To avoid potential incorrect estimations, these packets have been considered as lost which results with marginally higher packet loss results.
5. Results Analysis and Discussion

In this chapter the results for ETE Latency and Packet Loss obtained during the simulations, concerning the PMU data flow, are presented and analyzed for each scenario separately. The results for Jitter are presented in Appendix C.

5.1 Scenario 1.a and 1.b

This section presents the results collected during the simulation of the first scenario with 8 PMUs implemented in the network and without QoS schemes.

5.1.1 Normal Load (1.a)

- **End-to-End Latency**
  
  Figure 21 illustrates a graph representation of the End-To-End Latency for PMU packets when simulating the network under normal load. As observed in the graph, the latency grows more than exponentially in the first 20-30 seconds where all initializations in the network are performed and routing tables created. When the network configuration is entirely established, the traffic becomes steady and the PMU packets ETE Latency reach their peak value of 3.2 ms remaining constant for the rest of the simulation. The relatively low latency value is due to the absence of any other data traffic circulating in the network which provides the PMU packets exclusive right for the available link capacities.

![Figure 21 – Scenario 1.a, End-To-End Latency (normal network load) (image)](image)

- **Packet Loss**
  
  During the simulation of the first scenario, with normal network load, there are 360360 PMU packets transmitted in the network while the amount of PMU packets that arrive at the PDC is 358527. Consequently, the packet loss is equal to 1833 packets which correspond to 0.5% from the total amount of transmitted PMU packets.
5.1.2 Heavy Load (1.b)

- **End-to-End Latency**
  The results for the End-To-End Latency for PMU packets when simulating the network in *Scenario 1* with heavy load are presented in *Figure 22*. As observed in the graph, the latency curve develops in the same manner as in the previous case, except the fact that it becomes steady a bit later and its peak value reaches 4.9 ms. From there on it stays constant until the end of the simulation. Compared to the previous case, the ETE Latency increases with 53% but it is still under the tolerable margins that are between 20 and 30 ms. The increase depends on the presence of video traffic in the network which is estimated to 1.7 Mbit/sec per video unit.

![Figure 22 – Scenario 1.b, End-To-End Latency (heavy network load)](image)

- **Packet Loss**
  In this sub scenario, the results obtained for the PMU packet loss are corresponding to the results from the previous case. Namely, the total amount of transmitted PMU packets in the network is 360360 and the amount of arrived PMU packets at the PDC is 358527. This entails that the packet loss rate is 0.5%. Evidently, the presence of video traffic in the network does not result with increased packet loss regarding the PMU traffic.
5.2 Scenario 2.a and 2.b
This subchapter presents the results obtained from the simulation of the second scenario with 8 PMUs implemented in the network where QoS schemes are implemented in form of RSVP and MPLS.

5.2.1 Normal Load (2.a)

- **End-to-End Latency**
  The results from the second scenario concerning the PMU packets and their ETE Latency are presented in Figure 23. Similar to the previous scenario, the curve becomes invariable after approximately 100 seconds and its peak value is 3.8 ms. Compared to Scenario 1 the PMU packets latency increases with about 18%. It depends on the implementation of RSVP and MPLS protocols which results with longer packet processing times at the routers in the network.

  ![Figure 23 – Scenario 2.a, End-To-End Latency (normal network load)](image)

- **Packet Loss**
  In Scenario 2 with normal network load, the total number of transmitted PMU packets is 360360. The amount of received PMU packets by the PDC is 360055. Clearly, the difference is 305 packets which correspond to 0.08% from the total amount of transmitted PMU packets. Consequently the packet loss rate is 0.08%. Compared to Scenario 1, there is a clear improvement which indicates the role and the benefits provided by the implementation of RSVP.
5.2.2 Heavy Load (2.b)

- **End-to-End Latency**

Figure 24 depicts the progress of the ETE Latency curve during the simulation of the network in Scenario 2 with heavy network load. A minor increase is noticeable concerning that the peak value in this case is 5.1 ms, which is 5% higher in comparison to Scenario 1 with heavy load. The corresponding comparison between Scenario 1 and 2 with normal network load results in 18% increase of the ETE Latency in Scenario 2. This shows that, regarding packets ETE Latency, QoS schemes are more desirable and effective in networks where larger amount of traffic is present.

![Figure 24 – Scenario 2.b, End-To-End Latency (heavy network load)](image)

- **Packet Loss**

With the same rate of 360360 generated PMU packets, the amount of arrived packets slightly decreases to 360004 compared to the previous sub scenario. Accordingly, the number of lost PMU packets is 356 which is equivalent to 0.1% from the total amount of transmitted PMU packets. Thus, the packet loss in this sub scenario is 0.1%. While there is an evident enhancement compared to Scenario 1, there are roughly any differences in comparison to Scenario 2.a with normal network load.
5.3 Scenario 3
This subchapter presents the results obtained during the simulation of the third scenario with 16 PMUs implemented in the network along with Video and IP Telephony. The RTU traffic hasn’t been taken into consideration in this scenario. Traffic regulation is achieved by implementing RSVP and MPLS.

- **End-to-End Latency**
  The graph depicted in *Figure 25* presents the ETE Latency for PMU packets in *Scenario 3*. The presence of IP Telephony traffic in the network does not affect the PMU packets distribution significantly and their latency is 5.2 ms which is barely 2% increase compared to *Scenario 2*. It depends on the fact that in both scenarios same link capacity is allocated for the PMU data flow, which evidently is enough to keep the ETE Latency within acceptable margins.

![Figure 25 – Scenario 3, End-To-End Latency (No RTU traffic)](image)

- **Packet Loss**
  In this scenario, the network contains 16 PMUs. It results in 720720 PMU packets transmitted during the entire simulation. When the simulation ends, there are 720224 PMU packets that have arrived at the PDC. The missing 496 packets constitute 0.07% of the total amount of transmitted PMU packets.
5.4 Scenario 4
This subchapter presents the results obtained during the simulation of the fourth scenario with 16 PMUs implemented in the network and several QoS schemes. The RTU traffic has been taken into consideration in this scenario along with Video and IP Telephony.

- **End-to-End Latency**
  Figure 26 presents the development of the ETE Latency for PMU packets in Scenario 4. As observed in the graph the Latency peak value is 5.3 ms which is equivalent to 2% growth compared to Scenario 3 where RTU traffic was not taken into consideration. The obtained result is well below the predefined requirements for packets ETE Latency which is in the range between 20 and 30 ms.

![Figure 26 – Scenario 4, End-To-End Latency (with RTU traffic)](image)

- **Packet Loss**
The packet loss rate in this scenario is corresponding to the results in Scenario 3, 0.07%. It can be stated that additional RTU traffic in the network does not result in higher PMU packet loss rate.
5.5 Result Summarization

The ETE Latency results for PMU traffic acquired from all scenarios are well below the requirements for an IP Network with incorporated PMUs. A comparison between Scenario 1.b and 2.b with heavy network load points out that the use of RSVP and MPLS result in an efficient way of keeping the ETE Latency low. This effect is also noticeable in Scenario 3 and 4 where the network traffic is extensively increased, thus generating considerably more traffic in the network. Although the significant increase in network traffic, the ETE Latency only increases by 4% in total compared to Scenario 2.

As seen in Figure 27, the modeled network in Scenario 1 with no QoS schemes implemented is not able to maintain low PMU packet loss rate. Implementing RSVP and MPLS in Scenario 1, resulting in Scenario 2, lowers the amount of lost PMU packets drastically from 1833 to 305 PMU packets under normal network load and 356 PMU packets under heavy network load respectively. In both scenarios, the total amount of transmitted PMU packets in the network is 360360 in total.

The obtained PMU packet loss results from Scenario 2, 3 and 4 are clear indicators that the modeled networks in the respective scenario can effectively handle the amount of traffic present in them. There is a minor difference between packet losses in Scenario 2 compared to Scenario 3 and 4 although the total amount of network traffic is significantly increased in the latter two scenarios to 720720 transmitted PMU packets, Figure 28. It indicates the benefits provided by RSVP implementation in the network where the PMU packets have the same amount of link capacity reserved.
The important matter concerning jitter measurements are the variation they indicate on the ETE latency. As observed in the jitter graphs in Appendix C, after the jitter curve reaches its peak value, it remains constant. This is an important characteristic which implies that PMU packets arrive to the PDC in even intervals. If the jitter varied, it would denote that PMU packets have diverse ETE latencies, which is a consequence of inferior network stability. The simulations results are summarized in Table 6.

<table>
<thead>
<tr>
<th>Scenario/Metric</th>
<th>ETE Latency</th>
<th>Packet Loss</th>
<th>Jitter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scenario 1 (Normal Load)</td>
<td>3.2 ms</td>
<td>1833 (360360)</td>
<td>0.03 ms</td>
</tr>
<tr>
<td>Scenario 2 (Normal Load)</td>
<td>3.8 ms</td>
<td>305 (360360)</td>
<td>0.7 ms</td>
</tr>
<tr>
<td>Scenario 1 (Heavy Load)</td>
<td>4.9 ms</td>
<td>1833 (360360)</td>
<td>0.7 ms</td>
</tr>
<tr>
<td>Scenario 2 (Heavy Load)</td>
<td>5.1 ms</td>
<td>356 (360360)</td>
<td>0.7 ms</td>
</tr>
<tr>
<td>Scenario 3</td>
<td>5.2 ms</td>
<td>496 (720720)</td>
<td>0.7 ms</td>
</tr>
<tr>
<td>Scenario 4</td>
<td>5.3 ms</td>
<td>496 (720720)</td>
<td>0.7 ms</td>
</tr>
</tbody>
</table>

As observed in Table 6, it can be concluded that the obtained simulation results are relatively low. The reasons contributing to such an outcome are listed below.

- **Network Capacity**
  As already described before, the capacity in the network is pretty high considering that the bandwidth in the core network is 34 Mbit/s while the link capacity between access routers and core routers is 2 Mbit/s. Overall analysis provides that the highest amount of traffic, simulated in Scenario 4, corresponds to approximately 15% of the core network capacity.

- **Network Architecture**
  The network used during the simulations is not so complex and only consists of four core routers, representing the core network. This results in small amount of hops that each packet makes before arriving at its destination. In the current network, the maximum amount of hops that a packet does is 5. It implies that the packet is only processed by four routers while propagating the network.

- **Bandwidth Reservation**
  Considering the sufficient capacity in the network, satisfactory amount of bandwidth could be reserved for the data flows when implementing RSVP, approximately 10% over the theoretical maximum data rate for respective data flow.
Besides that, every data flow has its correspondingly required bandwidth reserved in every scenario where RSVP is implemented.

5.6 Further Research
In order to broaden the research conducted in this master thesis, and thereby get a more complete picture over the impact that QoS imposes in wide area networks, particularly the implementation of RSVP and MPLS, further investigations have been performed. As a consequence, two additional scenarios, 5 and 6, have been constructed with the network topology from Scenario 1 and 2 as a foundation. This also implies that QoS has only been implemented in the second additional scenario, Scenario 6. However, supplementary hosts, in form of 200 RTUs, have been added in the network resulting in increased total amount of network traffic. Table 7 summarizes the different data flows and their characteristics.

<table>
<thead>
<tr>
<th>Unit/Characteristic</th>
<th>Amount</th>
<th>Generated traffic per unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMU</td>
<td>8</td>
<td>19.2 Kbit/s</td>
</tr>
<tr>
<td>RTU</td>
<td>200</td>
<td>8 Kbit/s</td>
</tr>
<tr>
<td>Video</td>
<td>2</td>
<td>1.7 Mbit/s</td>
</tr>
</tbody>
</table>

In order to study the behavior of the PMU data under more extreme network conditions, three distinct simulations have been carried out for each of the two scenarios described above, where the overall link capacities in the network are varying between 2, 4 and 8 Mbit/s. In the first case, it is evident that the total amount of generated traffic is noticeably greater in comparison to the available capacity in the network, 2Mbit/s. Even in the second case, the entire traffic in the network exceeds the available network capacity of 4 Mbit/s. In the final simulation, the network capacity is sufficient in comparison with the total amount of generated traffic of approximately 6 Mbit/s. During these simulations the End-To-End Latency and the Packet Loss, regarding the PMU traffic, have been measured in the same manner as in the previous scenarios.

• **End-To-End Latency**
  The obtained results for the ETE Latency in Scenario 5 and 6 are presented in Figure 29 and Figure 30 respectively. In Scenario 5, the peak values for the ETE Latency are 46 ms with 2 Mbit/s network capacity, 10.6 ms with 4 Mbit/s network capacity and 6.4 ms when the total network capacity is 8 Mbit/s. In Scenario 6, the respective Latency values for 2, 4 and 8 Mbit/s network capacity are 12 ms, 10 ms and 6.4 ms. It can be noticed that the Latency does not vary drastically between the scenarios apart from the 2 Mbit/s simulations, where the difference is 34 ms. This deviation depends on the network instability and the lack of packet prioritization at the routers. When analyzing the results from each scenario separately it is evident that the decrease of network capacity results with higher End-To-End Latency.
Figure 29 – Scenario 5, End-To-End Latency

Figure 30 – Scenario 6, End-To-End Latency

- **Packet Loss**
  The Packet Loss rates that were measured during the simulations of Scenario 5 and Scenario 6 are summarized in Figure 31. In Scenario 5, with 2 Mbit/s network capacity, the Packet Loss rate for the PMU packets is 69.4%. For the same scenario, with 4 Mbit/s and 8 Mbit/s total network capacity, the Packet Loss values
are 21.9 % and 13.6 % respectively. The high Packet Loss rates depend on the lack of sufficient network capacity and packet prioritization. In Scenario 6, with total network capacity of 2 Mbit/s, the Packet Loss is 58.3 %. The corresponding Packet Loss values measured with 4 Mbit/s and 8 Mbit/s network capacity, are 0.03 % and 0.028 % respectively. The high packet loss in the 2 Mbit/s simulation depends on the insufficient network capacity compared to the total amount of generated traffic, approximately 3 times more than the available network capacity. However, the benefits of low packet loss provided by the implementation of RSVP and MPLS are evident in the latter simulations. In the second simulation, even though the generated traffic exceeds the network capacity of 4 Mbit/s, the PMU packet loss is still reasonably low due to the sufficient amount of reserved bandwidth in the network and the presence of packet prioritization.

![Figure 31 – Packet Loss, Scenario 5 and Scenario 6](image)

The results for End-To-End Latency and Packet Loss, measured in Scenario 5 and 6, are summarized in Table 8.

<table>
<thead>
<tr>
<th>Scenario/Characteristics</th>
<th>2 Mbit/s</th>
<th>4 Mbit/s</th>
<th>8 Mbit/s</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Latency</td>
<td>Packet Loss</td>
<td>Latency</td>
</tr>
<tr>
<td>Scenario 5</td>
<td>46 ms</td>
<td>69.4 %</td>
<td>10.6 ms</td>
</tr>
<tr>
<td>Scenario 6</td>
<td>12 ms</td>
<td>58.3 %</td>
<td>10 ms</td>
</tr>
</tbody>
</table>
5.7 TCP and UDP
To choose between TCP and UDP is often a difficult task. A major factor that influences the choice is the type of data which is sent. Depending on the requirements for the data, a few required characteristics can be established. The biggest trade-off between these two protocols is between speed and reliability. UDP counts as an unreliable but fast protocol, whereas TCP is reliable but also a slower protocol [16]. In this master thesis, there are between two and four distinguishable data flows with corresponding requirements depending on the scenario. The main focus is placed on the PMU data flow and how it traverses through the network. The PMU data flow needs both reliability and speed; this creates a dilemma.

In Scenario 1, there are no QoS schemes implemented, thus using UDP as the transport protocol is not the best choice, but it presents the opportunities to compare how QoS schemes upgrade the network performance. In case of an eventual congestion in the network, it is of outermost importance that PMU data is not completely lost and because of the lack of any QoS schemes in Scenario 1, the results will not be as positive as other scenarios. In Scenarios 2, 3 and 4, UDP, yet again, is used as a communication protocol for the PMU data flow. The main reason is the speed-advantages it provides. The reliability issue is now solely dependent on QoS where congestion is avoided through bandwidth reservation and prioritization. Another issue which might present itself by using TCP is the fact that TCP-sessions are created and shut down during a transmission. This process depends on what kind of data flow is using the TCP protocol. In the case of PMU data flow where the flow is continuous the TCP-session will be shut down when it is timed out or if a unit/link breaks down. This in turn will result in the creation of a new session, and if this is the case of numerous PMUs, it might cause congestion at the server site.

5.8 Assumptions
Even though the positive results from the simulations, there are some assumptions that have been made during this master thesis. Assumptions have been drawn regarding queue sizes in routers, packet sizes and transmission rates for RTU- and IP Telephony traffic. However, the respective packet sizes and transmission rates for RTU and IP Telephony are in this case not so decisive as long as they generate the desired amount of background traffic in the network.
6. Conclusions
The work performed during this master thesis has lead to an investigation of PMU traffic in IP based networks. This investigation has shown how the usage of QoS schemes, in particular RSVP and MPLS, can improve network performance. In order to accomplish a study on varied network environments, several network scenarios were created. The diversity in the scenarios enabled comparisons between simulation results, which in turn lead to a more complete analysis of the network performance.

The most important metrics in this master thesis are the End-to-End Latency and Packet Loss for PMU packets. The results acquired for the ETE Latency is well below the established requirements. This in turn indicates that the current network configuration can handle the present amount of traffic. An Improvement can also be seen in the results for Packet Loss. Clearly the QoS schemes used in the simulations also keeps the packet loss rates low and thereby contributes to an overall performance improvement. A critical factor to the positive simulation results, although the increased amount of traffic in the network, Scenario 3 and 4, was the use of RSVP. The conclusion to be drawn is that integrating additional PMUs in a network, while keeping the network performance within acceptable boundaries, is possible as long as adequate amount of bandwidth is reserved throughout the link paths.

Another important conclusion which has been established is that the current network, with implemented QoS schemes, has sufficient capacity to handle incorporation of additional units, namely RTUs and IP Telephones along with their respective traffic.

To additionally investigate the network capabilities, supplementary research has been performed where two extra scenarios were simulated. The objective with these scenarios were mainly to examine the minimum amount of link capacities needed without degrading the network performance and also to thoroughly investigate how the QoS schemes improve the network performance. The results show that by implementing RSVP and packet prioritization, the ETE Latency is kept low in all examined cases.

However, to maintain low Packet Loss values showed to be a bit more demanding. The usage of RSVP and packet prioritization was not solely enough, but the overall link capacities needed to be at least 4 Mbit/s in order to obtain acceptable packet loss rates.
6.1 Future Works
As a recommendation for future researches in this area, another more accurate simulation tool such as OPNET can be used to implement and simulate related network models. An appealing alternative network configuration which could be examined is the appliance of RSVP and MPLS solely on the PMU data flow. The point of interest is to observe the potential difference between implementing RSVP and MPLS on all data flows or on one particular data flow.

In terms of data security and integrity, Virtual Private Networks (VPNs) can be implemented in the network scenarios. It has not been an objective in this master thesis, thus the effects of it has not been examined.
References


[14] - David Lindow, Adrian Källgren, Jenny Florin, “Prestanda i en del av Svenska Kraftnätss kommunikationsnät”


# List of figures

| Figure 1 – Network Communication with QoS | .................................................. | 8 |
| Figure 2 – Electricity Market Overview | .................................................. | 10 |
| Figure 3 – Gridstat Architecture | .................................................. | 11 |
| Figure 4 – PMU Structure | .................................................. | 12 |
| Figure 5 – PMU Data Flow | .................................................. | 13 |
| Figure 6 – IP Network Overview | .................................................. | 15 |
| Figure 7 – RSVP Overview | .................................................. | 17 |
| Figure 8 – MPLS Overview | .................................................. | 18 |
| Figure 9 – Traffic Descriptor | .................................................. | 20 |
| Figure 10 – Traffic Profile for PMU Data Flow | .................................................. | 21 |
| Figure 11 – Flow Characteristics | .................................................. | 21 |
| Figure 12 – Method Overview | .................................................. | 24 |
| Figure 13 – Geographical Network Model | .................................................. | 28 |
| Figure 14 – Control Centre Overview | .................................................. | 29 |
| Figure 15 – Core Network Overview | .................................................. | 29 |
| Figure 16 – Subnet 1 Overview | .................................................. | 30 |
| Figure 17 – Scenario 1 | .................................................. | 32 |
| Figure 18 – Scenario 2 | .................................................. | 32 |
| Figure 19 – Scenario 3 | .................................................. | 33 |
| Figure 20 – Scenario 4 | .................................................. | 34 |
| Figure 21 – Scenario 1.a, End-To-End Latency (normal network load) | .................................................. | 36 |
| Figure 22 – Scenario 1.b, End-To-End Latency (heavy network load) | .................................................. | 37 |
| Figure 23 – Scenario 2.a, End-To-End Latency (normal network load) | .................................................. | 38 |
| Figure 24 – Scenario 2.b, End-To-End Latency (heavy network load) | .................................................. | 39 |
| Figure 25 – Scenario 3, End-To-End Latency (No RTU traffic) | .................................................. | 40 |
| Figure 26 – Scenario 4, End-To-End Latency (with RTU traffic) | .................................................. | 41 |
| Figure 27 – Packet Loss, Scenario 1 Vs Scenario 2 | .................................................. | 42 |
| Figure 28 – Packet Loss, Scenario 2 Vs Scenario 3 and 4 | .................................................. | 42 |
| Figure 29 – Scenario 5, End-To-End Latency | .................................................. | 45 |
| Figure 30 – Scenario 6, End-To-End Latency | .................................................. | 45 |
| Figure 31 – Packet Loss, Scenario 5 and Scenario 6 | .................................................. | 46 |
| Figure 33 – Network Model, Scenario 1 and Scenario 2 | .................................................. | 56 |
| Figure 34 – Network Model, Scenario 3 | .................................................. | 57 |
| Figure 35 – Network Model, Scenario 4 | .................................................. | 58 |
| Figure 36 – Scenario 1, Jitter (Normal Load) | .................................................. | 59 |
| Figure 37 – Scenario 1, Jitter (Heavy Load) | .................................................. | 59 |
| Figure 38 – Scenario 2, Jitter (Normal Load) | .................................................. | 60 |
| Figure 39 – Scenario 2, Jitter (Heavy Load) | .................................................. | 60 |
| Figure 40 – Scenario 3, Jitter (No RTU Traffic) | .................................................. | 61 |
| Figure 41 – Scenario 4, Jitter (With RTU Traffic) | .................................................. | 61 |
List of tables

Table 1 – Voltage Instability Assessment Requirements ..................................................... 22
Table 2 – Frequency Instability Assessment Requirements ................................................. 22
Table 3 – Oscillation Monitoring and Control Requirements .............................................. 23
Table 4 – Data Rate and Packet Size for Data Flows ........................................................... 31
Table 5 – Scenario Summary ................................................................................................ 34
Table 6 – Result Summary .................................................................................................... 43
Table 7 – Additional Scenarios, Network Characteristics .................................................... 44
Table 8 – Additional Scenarios, Simulation Results .............................................................. 46
Table 9 - Real Time Wide-Area Monitoring and Analysis – Phasor Data Requirements .... 54
Table 10 – Data Delivery Requirements ............................................................................. 55
Table 11 – PDC Requirements ............................................................................................ 55
Table 12 – Abbreviations .................................................................................................... 62
Appendix A, Requirements

Phasor Data Requirements

Table 9 - Real Time Wide-Area Monitoring and Analysis – Phasor Data Requirements

<table>
<thead>
<tr>
<th>Requirement Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Frequency data shall be collected at a minimum scan rate of 0.1 second (100 milliseconds intervals). Transmittal or communication from the frequency transducer to the data warehousing facility may take place on an asynchronous basis (i.e., need not be in real time). Sites with asynchronous transmission must have a minimum of 5 hours of local data storage to accommodate for data transmission failure.</td>
</tr>
<tr>
<td>• Each frequency data sample shall be appropriately identified as to Interconnection, source, and time of collection to the nearest 0.01 second. The time stamp shall be in Greenwich Mean Time (GMT or UTC).</td>
</tr>
<tr>
<td>• Synchronization of the frequency sampling intervals, time stamp information and any other time information required should be obtained from sources directly traceable to the NIST time source.</td>
</tr>
<tr>
<td>• Frequency data shall be collected to a resolution of at least +/- 0.001 Hertz (three decimal places)</td>
</tr>
<tr>
<td>• At each of the frequency transducer sites, a time error device shall be installed and time error shall be measured and transmitted. The time error shall be stored and uploaded to the central warehouse at the same rate as the frequency data. The requirement for triggering to collect at a higher rate shall not apply to the time error collection.</td>
</tr>
<tr>
<td>• A “first in, first out” (FIFO) buffer of at least six hundred (600) samples collected each 0.1 seconds (100 millisecond samples collected for one minute) shall be populated continuously for each Interconnection.</td>
</tr>
<tr>
<td>• Upon the occurrence of one of the trigger conditions (defined below) the FIFO Buffer and at least six thousand (6,000) samples collected each 0.1 seconds (100 millisecond samples collected for ten minutes) shall be achieved in a manner similar to standard frequency data for future access.</td>
</tr>
<tr>
<td>• Sufficient resources should be allocated to locally store fifty (50) triggered events per site.</td>
</tr>
<tr>
<td>• Options for increasing the sample period from ten (10) minutes to:</td>
</tr>
<tr>
<td>- Fifteen minutes, nine thousand (9,000) samples collected each 0.1 seconds.</td>
</tr>
<tr>
<td>- Thirty minutes, eighteen thousand (18,000) samples collected each 0.1 seconds.</td>
</tr>
<tr>
<td>• Trigger conditions should be flexible and programmable and are required to be independent for each site. At a minimum the trigger conditions should include the following classes of conditions:</td>
</tr>
<tr>
<td>- Frequency magnitude, high and low.</td>
</tr>
<tr>
<td>- Frequency rate of change magnitude, positive and negative, over one or more scan cycle.</td>
</tr>
<tr>
<td>- Manual request received from the Interconnection Frequency Monitor via direct electronic communications (ICCP or other direct, real time communications).</td>
</tr>
</tbody>
</table>
Data Delivery Requirements

Table 10 – Data Delivery Requirements

<table>
<thead>
<tr>
<th>Communication Message Types</th>
<th>Priority</th>
<th>Criticality</th>
<th>Security</th>
<th>Integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection Information</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Demand Information</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Periodic Information</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Low-speed Operations and Maintenance Information</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Text Strings</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Processed Data Files</td>
<td>L</td>
<td>M</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Program Files</td>
<td>L</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Image Files</td>
<td>M</td>
<td>L</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td>Audio and Video Data Streams</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
</tbody>
</table>

PDC Requirements

Table 11 – PDC Requirements

<table>
<thead>
<tr>
<th>Requirement Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Core Functionality</strong></td>
</tr>
<tr>
<td>Aligning data into a comprehensive data block.</td>
</tr>
<tr>
<td>Ability to accept data sources with different data rates.</td>
</tr>
<tr>
<td>Ability to handle missing and/or corrupted input data.</td>
</tr>
<tr>
<td>Ability to accept data sources in data format other than C37.118.</td>
</tr>
<tr>
<td><strong>Distributing data to various users</strong></td>
</tr>
<tr>
<td>Ability to distribute received data to multiple users simultaneously, each of may have different requirements on the data.</td>
</tr>
<tr>
<td>Ability to process and repack received data into different data rates from that of received.</td>
</tr>
<tr>
<td>Ability to repack data with different subset of data from the received data.</td>
</tr>
<tr>
<td>Ability to output data in other formats in addition to C37.118.</td>
</tr>
<tr>
<td><strong>Performance, History and Trouble Alarms</strong></td>
</tr>
<tr>
<td>Ability to log PMU Availability statistics</td>
</tr>
<tr>
<td>Ability to remote, configure and control PMUs</td>
</tr>
</tbody>
</table>
Appendix B, Network Models

Network model used in Scenarios 1 and 2

Figure 32 – Network Model, Scenario 1 and Scenario 2
Network model used in Scenario 3

Figure 33 – Network Model, Scenario 3
Network model used in Scenario 4

Figure 34 – Network Model, Scenario 4
Appendix C, Jitter Results

Graph representations of the obtained simulation results for Jitter are presented in this Appendix.

Scenario 1, Normal Network Load opposed to Heavy Network Load

- **Jitter (Normal Network Load)**
  
  *Figure 36* illustrates a graph representation of the Jitter measured in *Scenario 1* with normal network load. It is noticeable that after a short burst in the beginning of the simulation the jitter curve becomes steady and stays nearly constant. The Jitter value is approximately 0.03 ms.

- **Jitter (Heavy Network Load)**
  
  The results obtained for the Jitter in *Scenario 1* with heavy network load are depicted in *Figure 37* below. Compared to the previous case the jitter increases noticeably and reaches approximately 0.7 ms. This change is not so critical since the jitter value is constant. Constant jitter indicates that the network is stable and contributes with proper application functionality.
Scenario 2, Normal Network Load opposed to Heavy Network Load

- **Jitter (Normal Network Load)**
  Jitter measurements obtained from Scenario 2 with normal network load are presented in Figure 38. In this case the jitter, after it stabilizes, is approximately 0.7 ms which is evident increase compared to scenario 1 with normal network load.

- **Jitter (Heavy Network Load)**
  Figure 39 below, illustrates the results for jitter when simulating Scenario 2 with heavy network load. In this case the jitter reaches 0.7 ms and it involves a minor increase compared to Scenario 1 with heavy network load.
Scenario 3 opposed to Scenario 4

- **Jitter (No RTU Traffic)**
  Similarly to Scenario 2 the jitter curve reaches its highest value after approximately 200 seconds and stays constant until the end of the simulation, *Figure 40*. The peak Jitter value in this case is just below 0.7 ms which is generally equal to the measured jitter in the second scenario. This notification implies that the presence of IP Telephony traffic in the network does not influence the transmission of PMU packets in any way.

![Figure 39 – Scenario 3, Jitter (No RTU Traffic)](image)

- **Jitter (With RTU Traffic)**
  In the last scenario, the Jitter reaches 0.6 ms and stays constant until the end of the simulation which is depicted in *Figure 41*. It is evident that the presence of RTU traffic in the network does not have big impact on the PMU packets Jitter.

![Figure 40 – Scenario 4, Jitter (With RTU Traffic)](image)
## Appendix D, Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>ETE</td>
<td>End-To-End</td>
</tr>
<tr>
<td>PMU</td>
<td>Phasor Measurement Unit</td>
</tr>
<tr>
<td>PDC</td>
<td>Phasor Data Concentrator</td>
</tr>
<tr>
<td>TCP</td>
<td>Transport Control Protocol</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>RSVP</td>
<td>Resource Reservation Protocol</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multi Protocol Label Switching</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>NASPI</td>
<td>North American SynchroPhasor Initiative</td>
</tr>
<tr>
<td>SDH</td>
<td>Synchronous Digital Hierarchy</td>
</tr>
<tr>
<td>LSP</td>
<td>Layered Service Provider</td>
</tr>
<tr>
<td>WAMC</td>
<td>Wide Area Monitoring and Control</td>
</tr>
<tr>
<td>SMT</td>
<td>Synchronous Measurement Technology</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>FEC</td>
<td>Forwarding Equivalence Class</td>
</tr>
<tr>
<td>Eth</td>
<td>Ethernet</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>RTU</td>
<td>Remote Terminal Unit</td>
</tr>
</tbody>
</table>