Capacity Planning for Next Generation Utility Networks (PART 1)
An analysis of utility applications, capacity drivers and demands

Utility networks are going through massive transformations towards next generation conduits for new applications and critical data. Many of these networks have been around for years and have been adequately handling traffic demands, but as new services arise so does the demand for capacity. Networks that were built to sustain 100-200Mb/s of TDM/SONET/SDH traffic are now facing bottleneck situations and increased pressure to grow. The migration to packet based networks has introduced a plethora of new challenges to Utilities regarding capacity planning, efficiency, reliability and cost.

This paper describes capacity drivers for next generation utility networks and delves into detail about how to design these networks to meet the capacity need without sacrificing reliability or increasing cost. In the first part of this white paper, we will examine each of these services and its capacity contributions and then in the second part, explore how the combination of these services affect the network backhaul design. Separately we will do an analysis of a typical network and how to dimension the network capacity to be able to adequately handle these services and some factor of future growth.

Utility Capacity Drivers
Traditionally, private utility networks have carried mission critical applications – applications which are too sensitive to be carried on public operator infrastructure. These include voice, SCADA, teleprotection, operational services, and security related traffic. All of these services have been relatively low capacity in nature and even for larger networks with many substation and relay sites, the aggregation of all of these services didn’t yield a need for a high capacity backhaul pipe (larger than a standard DS3). Over the years, some services have grown in terms of scale and are requiring more bandwidth. New services have also been introduced into the network and are redefining how much capacity is needed. Some of the key applications and services, old and new, that are present in network planning and causing a huge spike in the capacity planning phase are:

A. Teleprotection (where low latency drives the need for additional bandwidth)
B. SCADA (migrating to packet-based protocols such as DNPoIP)
C. Traditional and Emergency Voice (moving to VoIP solutions)
D. Operational Services (remote access to an increasing number of field devices with increased frequency)
E. Corporate Networking including LTE Data (field staff expectation to be connected without interruption and FAN applications)
F. Security (both physical security systems and video surveillance backhaul)
G. Phasor Measurement Unit (PMU) Services (highly-accurate, real time sampled data – next generation SCADA)
Teleprotection:
Teleprotection is one of the most critical services for utilities and while each teleprotection circuit is inherently low in capacity (one DS0 or less), the method of transport of teleprotection can impact the necessary bandwidth. These circuits prevent failure and severe damage in the power network by transferring command signals between substations in the event of a protection trip. The circuits are extremely time sensitive to ensure that the faulty part is disconnected within the shortest possible time.

In terms of transport, traditional networks have carried teleprotection over TDM networks, where DS0’s were natively transported and service performance was guaranteed. As networks are migrating to packet based systems, the transport of these circuits over packet infrastructure can introduce issues with latency and delay. This occurs when the native signal is encapsulated and carried over packets in a process known as Pseudowire Emulation (PWE). PWE requires additional processing with added latency to the transmission of the signals, and one of the ways to counter the latency issue is to carry the signals over smaller frame size packets. While this can reduce the latency of the signal, it introduces additional overhead traffic to the overall payload. Since these circuits are small, the individual addition of unusable overhead traffic is fairly insignificant but from the total network standpoint, it can be noticeable. The capacity requirements per substation can vary significantly depending on the number of Teleprotection channels required. Smaller substations might only require a handful of channels while busy and high voltage substations could have as many as 75 channels terminating at the site.

Traffic Requirement per substation: ~300kb/s to 10Mb/s per substation.

Supervisory Control and Data Acquisition (SCADA):
SCADA traffic represents the command and control network of the utility and like Teleprotection is inherently very low in capacity but high in importance. SCADA is used to both monitor and control how the power system operates and provides operating status and alarms when abnormal conditions exist. This traffic provides data on the characteristics of the network that allow the utility to operate more reliably while also lower operating costs because of real time problem detection and resolution. It is the real-time dashboard of the grid, and hence is mission-critical.

Traffic Requirement per substation: ~300kb/s per substation.

Traditional and Emergency Voice:
Utilities still maintain private networks for their internal and mission-critical voice communications including traditional push-to-talk (PTT) mobile radio, private branch exchange (PBX) lines, and newer voice systems like VoIP and LTE. Hardened, private infrastructure ensures mission critical voice is available in emergency situations. Sizing the network for voice applications requires understanding current requirements and ensuring there is adequate space for future services and users. In terms of capacity, networks are designed for peak load since while the usage of voice is intermittent and not as frequent as in commercial LTE networks, the requirement can increase in cases of emergencies or if there is aggregation at the site.

Traffic Requirement per substation: ~1Mb/s to 3Mb/s per substation.
Operational Services:
Operational services include data access applications like metering, fault reporting and event analysis, which are all individual low capacity services but once aggregated, can become a large consumer of available bandwidth. This is especially true of metering services such that if the requirements change to include more meters in the network or more frequent polling of meters are desired, the increase in bandwidth also increases exponentially. While many utilities offload metering traffic to public networks, for security reasons, more and more are looking to keep this traffic on their own networks.

Traffic Requirement per substation: ~10Mb/s per substation.

Corporate Networking:
With the availability of Ethernet pipes on a private network, applications and services that sustain the corporate environment will increase. This includes standard LAN services, Internet connectivity and connectivity to link substations together. Traditionally this traffic has resided on public networks however access to a high speed private network offers a lower cost and more reliable option and many utility networks have a growing volume of corporate traffic. The bandwidth of this type of traffic can vary depending on the type of applications and these services are often times the lowest in priority but are still very capacity hungry.

In some cases where fixed corporate services are not possible, utilities would benefit from mobile broadband services. This is especially true in some of the remote parts of the networks where connectivity is necessary for utility personnel or other applications like field area networking (FAN). Currently, utilities lack dedicated spectrum for such services. Despite this, some utilities are forging alliances and partnerships to gain access to LTE spectrum for broadband communications. In these cases, network wide bandwidth can be difficult to plan since capacity requirements will depend on site density, spectrum availability, and LTE network design. Regardless, mobile data can drastically increase bandwidth requirements on utility transport networks.

Traffic Requirement per substation: ~10Mb/s per substation.

Security:
Security might be the single largest driver of capacity in utility networks today and the most bandwidth intensive security application is surveillance video. With the need to protect critical infrastructure and meet new regulations, use of surveillance cameras has risen. Networks need to support multiple, often high definition, cameras per location - each capable of 1080p resolution and also refresh and operate at a rate of 60+ fps. Newer cameras also offer pan-tilt-zoom (PTZ) capabilities allowing complete remote control of the camera. Each of these types of cameras can require up to 6Mb/s of sustained bandwidth. Utilities with thousands of substations, generation sites, and other facilities will demand ultra high capacity networks and will need to be carefully planned and engineered to ensure capacity demands of worst case emergency scenarios are met.

Traffic Requirement per substation: ~25Mb/s per substation.
**Phasor Measurement Unit (PMU) Services**

PMU sensors give utilities additional details about the performance of the network and tracks power quality at a very high resolution by streaming real time data as opposed to collection and transmission over time intervals. PMU’s are considered the next generation of SCADA because of its increased level of granularity and details and will eventually become one of the most important data sources in next generation power networks. Comparing the data resolution of PMU’s to SCADA, while SCADA typically collects 1 sample every 2-4 seconds, PMU’s collect 10-60 samples per second and measure both magnitude and phase angles of a phasor signal (SCADA only measures magnitude). The adoption of PMU’s in a network is growing and they will initially coexist with SCADA in the network but eventually PMU’s will remain. Designing a PMU network can also affect the bandwidth the services require and in terms of PMU design, there are two architectures – central concentration and local concentration. In a central concentration architecture, PMU’s forward data to a main control site while in a local concentration architecture, PMU’s provide primary data to the local substation and then a separate signal is sent from that substation to the control site. The following table shows an extrapolation of traffic depending on the architecture for local versus central concentration.

![Figure 1 – PMU bandwidth requirement for central office.](https://selinc.com/solutions/synchrophasors/report/115281/)

The bandwidth estimates show the approximate bandwidth required at the control site for each of the architectures. Also, based on the size of the network, the number of PMU’s in a fully-deployed network can easily exceed 500.

**Traffic Requirement per substation: ~3Mb/s to 11MB/s**

---

Capacity Planning for Next Generation Utility Networks (PART 2)

Capacity planning guidelines for utility transport networks

Knowing the traffic requirements from Part 1, we can analyze a sample network and see how the individual services contribute to the total required network capacity. Figure 2 shows the sample network which includes nine substation sites and one main control site. Rings are the preferred topology for utilities, due to their fault tolerance, and allow for more complex capacity planning scenarios. Figure 2 also shows the per site capacity required for each of the applications we identified in the network. Several of these applications have a range but in order to keep the analysis simple and conservative, we will use the lower-end range of each of the requirements.

![Sample network diagram and capacity requirements](image)

<table>
<thead>
<tr>
<th>Service</th>
<th>Capacity Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Teleprotection</td>
<td>300kb/s</td>
</tr>
<tr>
<td>SCADA</td>
<td>300kb/s</td>
</tr>
<tr>
<td>Voice</td>
<td>1Mb/s</td>
</tr>
<tr>
<td>Operational Services</td>
<td>10Mb/s</td>
</tr>
<tr>
<td>Corporate Networking</td>
<td>10Mb/s</td>
</tr>
<tr>
<td>Security</td>
<td>25Mb/s</td>
</tr>
<tr>
<td>PMU</td>
<td>3Mb/s</td>
</tr>
</tbody>
</table>

Figure 2 – Sample network diagram and capacity requirements.

Site 1 represents the control site where most services originate and terminate. Traffic loading for each site is calculated by aggregating traffic for all the applications running at that site (per the table above). Traffic loading for each microwave link is calculated by aggregating traffic flows from each site to the control site that traverses the link. Under normal conditions, traffic from each site will follow the shortest path to the control site, assuming a basic IP network transport scheme. Based on that, traffic loading for each link is shown in Figure 3. The green bars represent the density of traffic as you move closer to the control site and represent how different links can require a different capacity based on their proximity and route to the control site.
It is important to note that the traffic loading should not be confused with network capacity. The traffic loading represents what the per site and link loading will be based on the services running through the network. The necessary network capacity is calculated based on traffic loading, failure scenarios and future growth factors. This will be covered a little later.

The proper dimensioning of each microwave link needs to consider additional traffic loading under failure scenarios. In a ring topology, a failure on one of the two links feeding the control site (Link 1 or Link 10) represents the worst-case scenario for traffic loading as it shifts the traffic from all remote sites to the other link feeding the control site. Figure 4 below shows traffic loading for each link after a failure of Link 10. In this case, Link 1 will need to handle traffic from all remote sites.
Similar to Figure 3, the red bar represents the density of traffic around the ring and once again, the loading increases drastically as you approach the control site. In comparison to the loading under normal operation conditions, the per link traffic loading changes significantly. This is why the necessary network capacity has to take the traffic loading into consideration but it cannot be the exact same as loading. With ring systems, link and network capacities need to be based on worst case failure scenarios, so in this case, the loading impact of failover should be considered.

It is also important to dimension each microwave link so that it operates without congestion, no more than 80% of its capacity, under the worst-case failure scenario. This helps provide optimal performance for delay and jitter sensitive applications under failure scenarios. For example, in the sample network, the worst-case traffic loading on Link 1 is ~452 Mb/s. Therefore, it should be designed with a minimum capacity of 570 Mb/s (excluding growth); this ensures that even with a utilization factor of 80%, the link can handle the necessary loading of the link.

Since failover can occur over any link, you have to consider the worst case scenarios and in ring systems, that would represent the two links closest to the control site. So far we’ve considered a failure over link 10, which adds the highest loading burden on Link 1. Another scenario to consider is a failure over Link 1, in which case the traffic would traverse in the alternate direction and the major traffic loading burden falls under Link 10. In fact, in this second failover
scenario, the traffic loading per link becomes a mirror reflection of the loading we just calculated. This is because the sample ring network provides symmetry in terms of sites and routing to the control site. In this latter calculation, you could rotate the diagram shown in Figure 4 digram by the y-axis.

Another factor to consider when dimensioning the microwave links is the anticipated growth in network size, by adding spur links or subrings for example, as well increasing traffic demands of the existing applications or new applications. Growth factors can be included in the initial design of the links by reducing the load factor under worse case failure from 80% to 60% or less. Alternatively, the link design can be modular allowing for incorporating additional RF channels based on future demands. Considering utility networks are deployed to last at least 15 to 20 years, having a growth factor is necessary. It might increase the amount of unutilized bandwidth but gives the network traffic loading elasticity in case of increased demand or growth. Typical growth factor variables range from 15-20%.

Given the above analysis and considerations on how to properly dimension traffic, we can summarize the equation for link capacity as follows:

**Link Capacity = (Worst Case Load / 0.8) x Growth factor**

This equation demonstrates the relationships between the traffic loading, utilization and future growth. If we apply this equation to the links (assuming a 20% growth factor) in the above sample network, then the per link capacities required for this design are:

- **Link 1 Capacity:**
  
  \[
  = (452 \text{Mbs/.8}) \times 1.20
  \]
  
  = 675Mb/s

- Similarly:
  - **Link 2 Capacity:** 603Mb/s
  - **Link 3 Capacity:** 527Mb/s
  - **Link 4 Capacity:** 452Mb/s
  - **Link 5 Capacity:** 377Mb/s
  - **Link 6 Capacity:** 377Mb/s
  - **Link 7 Capacity:** 452Mb/s
  - **Link 8 Capacity:** 527Mb/s
  - **Link 9 Capacity:** 603Mb/s
  - **Link 10 Capacity:** 675Mb/s

You can see the symmetry in the above capacity requirements, which follows the requirements of failover in case the closest links to the Control site fail. The above capacities represent the minimum per link capacities needed to ensure adequate bandwidth under normal operating conditions, worst-case failover scenarios and to account for growth.
Summary:
Utilities require ultra-high capacity networks to keep up with growing volumes of mission critical data. While “backbone” links in older networks were designed with 50Mb/s, newer networks can easily require a minimum of 300Mb/s, and upwards of 1Gb/s. Factors such as the size of the network, network topology, failure scenarios, the volume of services and anticipated growth will affect these estimates. This paper showed a typical ring configuration and used some typical traffic loading assumptions in order to simplify the calculations and provide a baseline for calculating the network link capacities. This analysis can and should be extended to other configurations and can easily be adjusted to fit either different network topologies, different traffic loading of individual services, or a combination of the two. The methods and formulas that were used can still be applied to any type of network and adjusted accordingly.