SERVICE DESCRIPTION
IP Networks and ICT

version: 0518v1

Disclaimer

The Service Description, provided herein, is intended for the confidential use of the designated recipient(s) only. It may contain confidential and/or privileged material. Any transmission or dissemination of the Service Description or its information is strictly prohibited without BaseN´s prior permission.

Welcome to the BaseN Service Description

The BaseN service is a next generation SaaS suite that enables you to gather system, network and cloud measurement data and arrange the information in a context that is relevant to you and your customers. The BaseN service displays the data in an easily understandable, concise and relevant way - real time and historical. A unified view of status and performance can be seen at a glance, not limited only to infrastructure, but also applications and services, such as VoIP.

The BaseN service can be easily integrated into existing monitoring and management operations. Based on open standards, and offered as SaaS, it has comparatively low entry costs. It will help to significantly reduce overall costs by improving performance and fault management with SLA assurances, spotlight where additional capacity will soon be required, as well as highlight over-provisioning where usage can be increased without additional cost. The BaseN service provides system monitoring and measurement on a detailed level to enable early corrective action and immediate attention to problems, as well as real time and historical information for capacity planning.

Company Profile

BaseN is a privately held Finnish SaaS provider established in 2001. It was founded by a team of network specialists with years of experience from both the operator and the enterprise world. The company has a strong focus on design, optimization and management of networks. Company headquarters is in Helsinki and commercial offices are in Amsterdam, and in Sunnyvale, California. These local entities are fully owned subsidiaries of BaseN Corporation.

BaseN focuses on next-generation technology, providing services to enterprises and service providers in an accurate and cost effective way.

Differentiating Features

The differentiating features of the BaseN service are: scalability, fault tolerant architecture, broad multivendor support, easy adding of equipment and service templates, the ability to monitor anything that can send us data, and low entry cost as a cloud-based SaaS service.

BaseN's massively scalable, fully clustered and distributed architecture provides a united view of the entire monitored environment. Its grid architecture enables it to process millions of measurements per minute and makes it highly fault tolerant - able to lose 50% of its system infrastructure without service interruption.

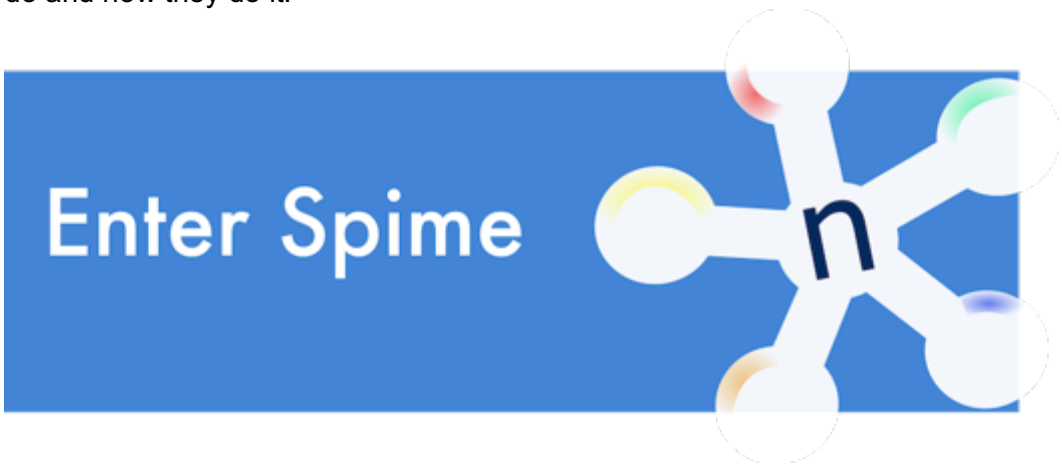
Device templates are at the heart of BaseN monitoring. We have over 1800 templates in our library. As you add new equipment, BaseN can provide new templates quickly - meaning you don't have to wait for a general software release to add to your monitored environment. BaseN can collect measurement data and status information actively (SNMP or other means) or passively via Syslog messages, SNMP traps, or email reception. We can monitor smart meters, home energy devices, credit card readers, solar panels and mobile radio/base stations, in addition to network and data center devices. The BaseN service can combine IP, IT, ICT, and even energy monitoring into one unified view.

Offering BaseN as a cloud-based always-on Software as a Service enables low entry costs and no capital expenditures. A one-time fee and low monthly charge are all the costs incurred in running the BaseN service, available to run in public or private/dedicated cloud.

The BaseN Platform

Architecture and Design Principles

BaseN is a mature Software as a Service (SaaS) and Platform as a Service (PaaS) provider, launched and in continuous development since December 2001, providing an extremely scalable, fully distributed, resilient, secure, and combined real-time monitoring and control platform for ICT, M2M, and IoT combined. BaseN provides new ways to capture, store, process, analyze, visualize, and control extreme volumes of things and data real-time, which enables next generation digital businesses to greatly improve what they do and how they do it.



At the core of the BaseN design philosophy is the concept of Spime, a logical incarnation of any thing. Spimes record and manage the full lifecycle of their physical representations as physical hardware and support software come and go. As such an object can be considered a Spime when all of its essential programming is managed in the cloud. The Spime concept was originally crafted by the author Bruce Sterling as a neologism for a futuristic Internet of Things object (see http://en.wikipedia.org/wiki/Spime).

Spime is patented by BaseN and the next generation extension of Digital Twin: US Patent (Pending) # 20170139788 (https://patents.google.com/patent/US20170139788A1/en) A Spime is the complete logical software description and mastering reflection of a physical object, typically a device or any other entity that performs a function, or series of functions, in a digital service. The Spime is defined and conceived before the appearance of its physical counterpart. In this sense, a Spime is independent of its physical representation, which can come and go and be easily replaced.

Grounded at the core of BaseN's pioneering distributed computing platform design philosophy and architecture, Spime enables the extreme levels of fully automated adaptability, sustainability, scalability, reliability, and security. These are all so critical elements in the future digital world of connected objects, but something that conventional data process, conventional storage systems and conventional service providing systems simply cannot cope with sufficiently well.

Because the core of BaseN platform's operational nature is fully based on a Spime architecture, it lends itself to fully enabling digital services which evolve and which have the capability to change over time. This is opposed to static instances of services, such as conventional software designs that need to be manually redesigned and re-launched whenever a change is needed.

Examples of components and entities defined and managed by Spime:

- Devices and device types and versions
- Device attributes and roles and relationships
- Device communications and security protocols
- Device and component control and configuration management functions
- Accounts and account data, all user interaction data, and security
- Data storage systems and failover mechanisms
- Data and analytics processing and computation components
- Software versions and attributes
- Presentation, portal, and end-user experience technologies, graphing engines and formats
- External API types, API versions, and systems communications with external and 3rd party ecosystem components
- All components and aspects of the BaseN platform itself

Additionally, BaseN provides a solution known as “Spime Enablers”, to drastically shorten time to market for (3rd party) devices and components that have not yet been upgraded to communicate via standard means over the Internet. BaseN has a series of options for customizing, deploying, and pairing Spime Enablers with such legacy devices and components.

The BaseN Platform Operating Environment (BPOE) is a stable, optimized and hardened Linux based operating system that runs on top of bare metal hardware providing a reliable layer for the BaseN platform software to run on. The platform itself is deployed with rigorous version control, security rules and demarcation points. It also includes a high level of automation, auto-discovery and self-configuration making new or incremental installations fast and simple.

The BaseN platform is highly agnostic to which specific hardware platforms it can be installed and run on and we support a range of both virtualized and non-virtualized options. For example, our platform software currently runs on ScLinux (ScientificLinux) but we can also fit our agent software on an SD card, such as the RaspberryPI. The exact server models, versions, and configurations we run on changes fairly quickly as these keep evolving rather rapidly. Please consult your designated BaseN representative should you wish to have detailed and up to date information about these environments at any given point in time. Also note that if for example servers are used for long-term data storage, memory and disk allocations are adjusted accordingly.

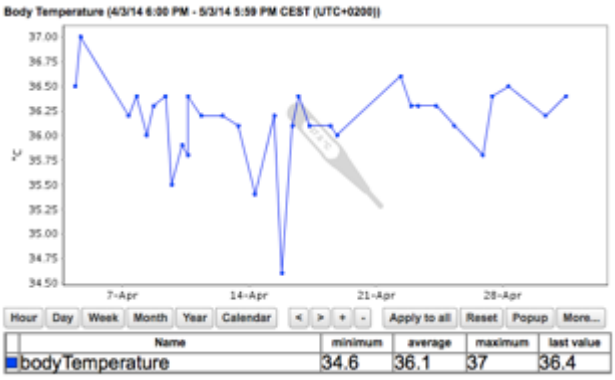
The platform is designed for multi-tenancy from the start. It provides secure Spime containers for customers for their own and their customers’ things in massive scale.

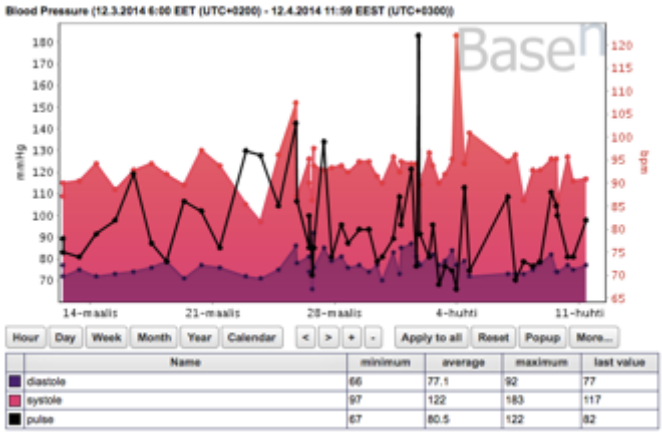
Agents or microagent units perform measurement and control functions. Agents are commodity servers (COTS) that support a large number of standardized data protocols; they are installed on or near the device layer and typically manage from hundreds to tens of thousands of devices. Microagents are based on API communications and allow a range of implementation options by embedded devices to nanocomputers monitoring smaller targets.

The core of the platform consists of data reception and storage components optimized for scalability, high volume and replication. All components can be added or removed on the fly, allowing both reception capability and storage period to be expanded as required.

The services layer that refines the data to produce exported signals, visualizations, configuration logic, and user interfaces, is similarly based on a dynamic service scheme and expands to meet the needs. The platform standard user interface is web based. An adapter based authentication and multi-layer access

scheme allows for granular per user or group visibility into data. The user interface, the measurement and export logic are programmable, and the external API permits specialized interfaces (e.g. systems integration or tablet/phone apps) that can for example access measurements, store data or control remote equipment.





In addition to being able to visualize data collected within the BaseN platform on a very granular level, BaseN also provides several alternatives of open and easy to use northbound APIs (including REST and JDBC) for obtaining not only fault and performance management data but also the raw measurements for external use, and customers may utilize all the rich analysis capabilities of BaseN platform in addition to their own. Customers may also subscribe (listen) to certain channels and choose to receive data in real time for those channels as it arrives from devices.

The BaseN platform also provides a container framework, boasting millions of full-fledged virtual computers capable of executing complex programs, Spimes, in various programming languages. These Spimes have access to all historical data and combined parallel processing power of the BaseN platform and can execute a multitude of fine tuned control functions in IoT environments.

Each Spime created and maintained in BaseN platform has full version control and rollback capabilities, including complete audit trail.

The BaseN platform is capable of control functions such as distributed software upgrades, complex end-to-end network configuration, power consumption control based on time of use pricing and for predefining heating cycles, managing AC and fans based on in-room CO2 levels, engine optimization through adjustment of car settings based on weather data, automated worksite gate management, healthcare crew dispatch based on real-time patient data, just to name a few examples.

BaseN microagent protocols have also been developed for automatic distribution of computing and storage resources, enabling seamless operation of Spimes both in local, millisecond-grade agents as well as in a centralized BaseN data centers with thousands of CPUs. The Spime master objects, however, always reside in BaseN platform and are automatically delegated to local microagent devices when needed.

BaseN's framework for control functions supports completely "headless" devices as well as highly sophisticated devices with local intelligence alike, and will be fully supported in the my.basen self-provisioning service.

BaseN
Device Data Flows
END USERS
WEB SERVICES
Customer Portals
End-user Portals
Content Manager
InSite Maps
Issue Manager
Report Manager
EXPORT SERVICES
Alerts SMS/Email/API/...
Inventory
Measurements PDF/XLS/image
Reports PDF/XLS/SQL
Client Output
Client Input
Device input
Device Control
Coordinating Logic
COMPUTATION SERVICES
AutoDiscovery
Configuration Information
User Management
Visualization
Map Tile Service
Report Manager
Issue Correlation
User Information
Events & Alerts
LONG TERM STORAGE
DATA RECEPTION
AGENT BASED DATA COLLECTION
DIRECT CONNECTION
Customer premises
End-user premises
End user: micro-agents, utility provider devices
Industrial customer: any supported IT, networking, telco devices
* Distributed computing service environment
* All components redundant, plus whole cloud redundancy
* Components added on the fly
* Located in BaseN data centers or customer premises
* BaseN/customer premises
* Redundancy - min. 2
* On-the-fly expansion
* Local buffering of data
A Alternatively, devices can communicate to a web API (directly or through a network enabled microagent).
B External applications and apps can poll customer device state through a front-end API.
C Customizable logic can combine external input, device input, and computation services to control a device or join the platform data flow.
1 Device measurements are collected by locally installed Agents.
Agents are redundant and cache their data in case of outages.
2 Agents relay their measurements to redundant data reception services.
Data reception hands the data over to long term storage.
3 Multiply redundant, sharded, dynamically expanded storage retains raw data for years.
4 Data reception also communicates to analysis services watching for exceptional situations.
5 Event services inform active monitoring applications in the BaseN Platform portal of the issues.
6 Alerting services produce a notification to send to the client or their issue management.
LEGEND
Agent
Cloud Service
Application Service
Data Export Service or Interface
Agent
Logger
Storage Unit
Configuration Storage
Web Content Provider
API
Web API

Unified Overview of the Entire Monitored Environment

Location Map and Real Time Alerting

The Location Map gives a real time overview of the operational status of, for example, an entire network. Devices are automatically placed on the map based on location details provided by configuration of the device, or by importing location details for each device. Location information can be further refined by latitude/longitude for each site. The map underlay contains visual information down to street/building level. Devices and sites are automatically connected based on layer 3 information (IP networks/subnet details). Each site containing more than one device can be zoomed into and local network layout visualized. The overview map shows link status between locations, as well as site status.

A red line on the map indicates a problem on the link between two sites. Clicking on the link brings up a separate window containing device and link information and details of the problem. For network operations this means that one screen provides the overview status of the entire network. The network operator no longer needs to page through many screens to see the status of the whole network. The need for fewer people to watch for alerts enables the redeployment of personnel to other projects, thereby increasing productivity without increasing head count. Texts and emails can also be used to notify operators of alert conditions.

The overview gives a quick summary of the state of the network and services. Green indicates normal operations and non-critical states. Yellow, orange and red indicate alerts and issues of varying severity. The overview enables you to drill down quickly to individual issues (locations or devices) and identify the root cause of the problem, thus substantially reducing response times. Map overviews can be customized to reflect different KPIs, such as availability, MOS score or any other critical KPI. This flexibility enables you to adapt the BaseN service's functionalities for your and your customer's needs. Furthermore, BaseN's capability to correlate, in real time, a significantly larger amount of information than traditional monitoring tools enables the NOC operator to be alerted to and pinpoint were service degradation occurs before customer impact.

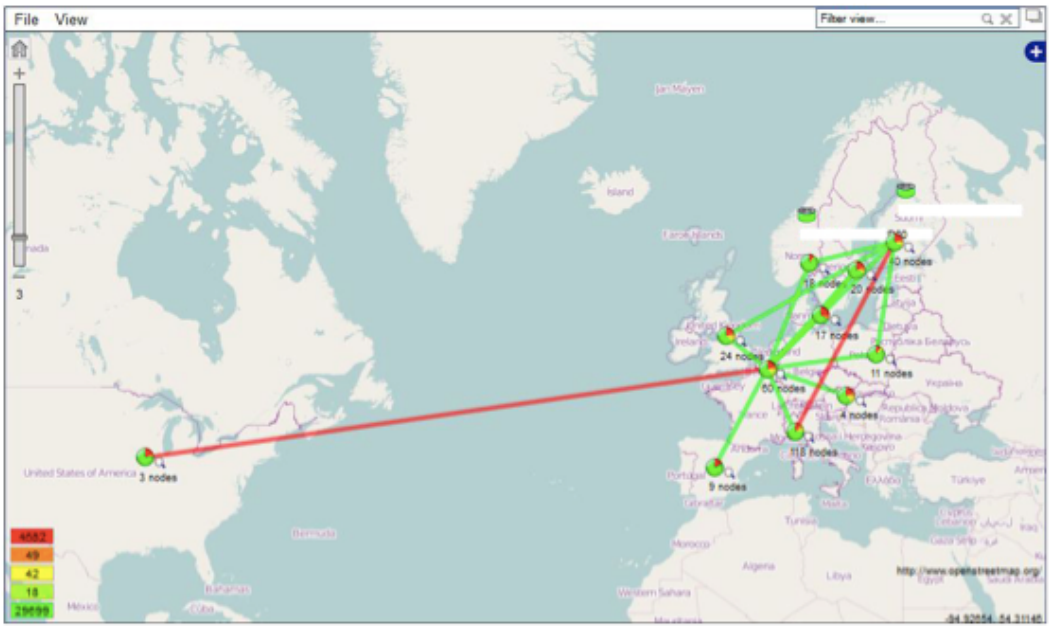


Illustration 1: Example of LocationMap Overview

Alert Information

The LocationMap in Illustration 1 indicates that there is an alert on the trans-Atlantic network connection. Clicking on this line brings up the details shown in Illustration 2. The blue banner at the top contains the network name, in this case a specific IP address. Vlan10, a private virtual local area network, has exceeded the utilization threshold percentage and alerts that the average utilization for the last hour has been 96.5%. Further details for this alert are found by clicking on the alert tab, as shown in Illustration 3 below.

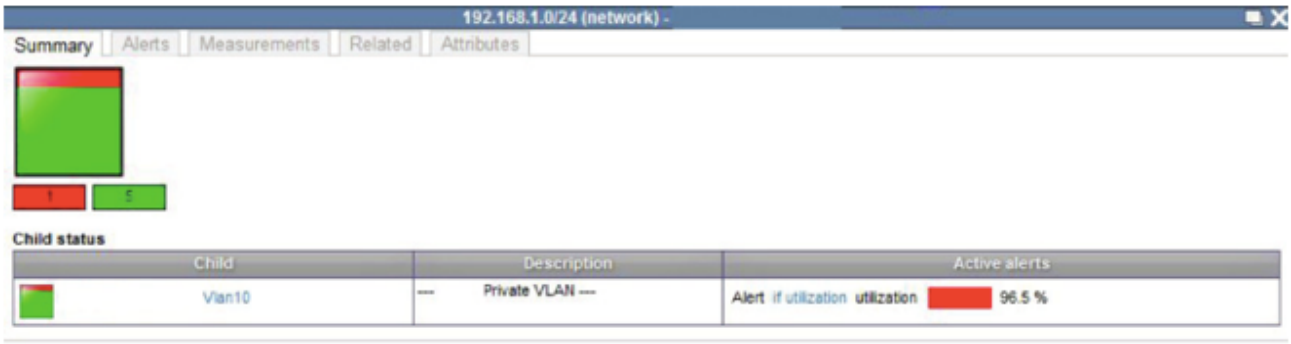


Illustration 2: Alert Detail from Clicking in Link Between Sites

Illustration 3 provides further insight into the alert condition. Here we see that the high utilization occurs between 9 and 10 am - which could be when most users are logging into the system. Analysis can compare the daily view with historical details for this measurement, which can be found by clicking on the page name shown under the Page heading. If historical utilization between 9 and 10 am is not comparable to the alerted condition, then the network operator can begin looking for the cause of the high utilization, before the link goes down. Or if historic utilization shows this link running at near full capacity all the time, then this provides information for capacity planning.

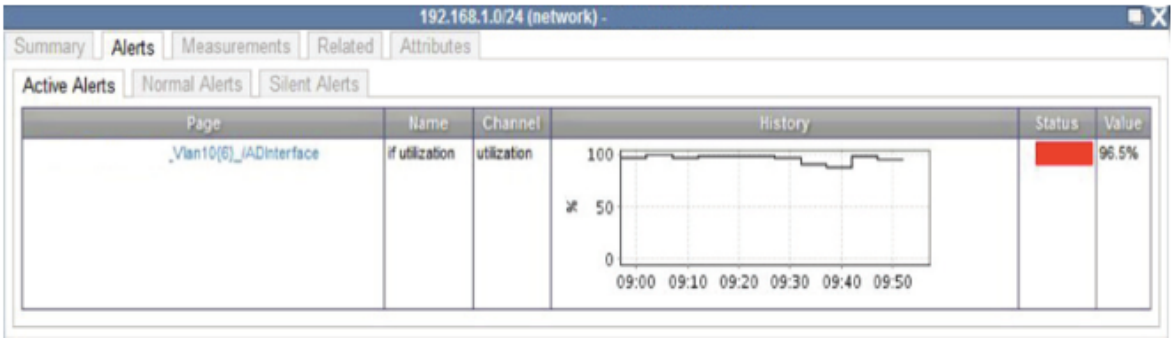


Illustration 3: Active Interface alert

Root Cause Analysis and the LocationMap

Since connectivity information is available in the Location Maps, it is used for Root Cause Analysis (RCA), using a 'root cause' filter to analyze dependencies between nodes. The 'root cause' filter is part of the default filter set.

For root cause to be enabled, the network needs to have one or more root cause roots configured. The root cause acts as the base of the dependency tree; they will never be silenced due to root cause analysis.

Categories of Root Cause Devices:

Automatic - The node type is automatically detected. This is the recommended setting for most nodes.
Root - Root of the network - this node can never become silent due to root cause analysis. It is part of the root cause logic as a device on which other devices are dependent. You need at least one of these in a network to enable root cause analysis.
Leaf - Think of this node as a leaf. No nodes depend on this node. Most servers are a leaf. Multi-homed (non routing) servers should be marked as a leaf. A node is automatically treated as a leaf if it has only one link into the network.
Hub - Hub is usually a node that can't be measured. All neighbors of a hub are treated as neighbors of each other. Layer3 networks and non-measurable switches are examples of hubs.
Node - Default type for network elements. Other nodes can depend on this node.
Ignore - A node that can't be part of a root cause analysis. It is neither depended upon and nor traversed through. It is not recommended to create islands of "ignore" nodes or islands that do not have a 'root'. When all the nodes on an island are down, these isolated nodes are all silenced and no alerts are sent.

See the roles in the illustration below from a BaseN Location Map: specific icons - Root, Ignore, and Hub - indicated these roles, others are indicated by the root cause analysis relationship to other nodes - automatically detected as Isolated or Leaf.

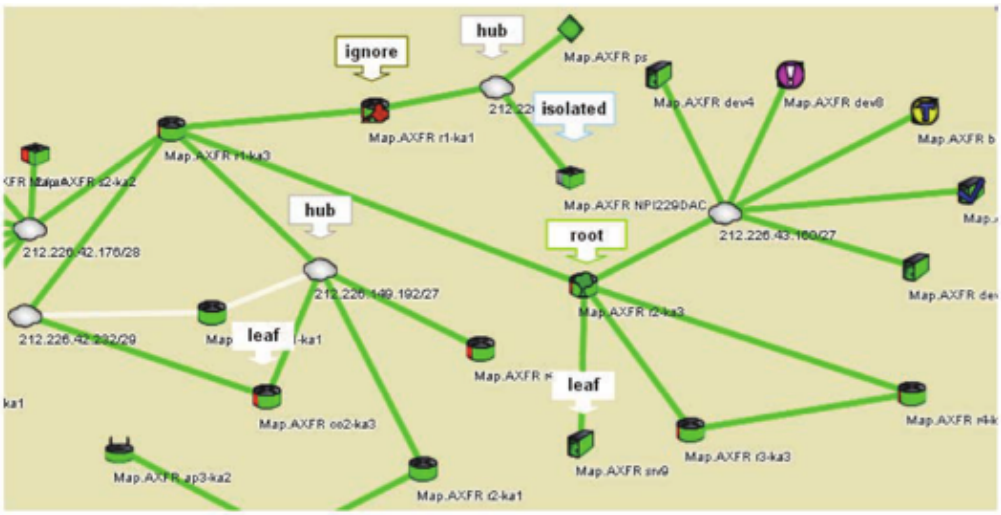


Illustration 4: Root Cause Analysis

IssueManager and Root Cause Analysis

The BaseN IssueManager provides an operational status overview of all current alert conditions, as well as problem details. Issues are automatically ordered according to status and priority as defined by the user during installation, and new alerting thresholds and priorities are easily changed by the user as needed.

Each Issue contains relevant detail concerning the alert condition such as name, time the alert occurred, location details and customer information. The information is configurable according to the user requirements. In addition to the information above, other details can be automatically added to alerts and issues, such as SLA requirements. The details in the IssueManager can also be linked to a ticketing system, and the Issue updated with relevant ticket details for problem resolution. Each Issue contains a link to the BaseN page where additional alert information can be found.

The IssueManager also displays root cause identification and clear alerting of source problems. BaseN's root cause analysis suppresses secondary alerts where measured elements depend on other elements. This eliminates secondary alerts being created on dependent objects that are not the real root cause of the problem. Root cause analysis can be either automatic (based on discovery of node relationships), explicit (based on single node or measurement characteristics) or manually configured.

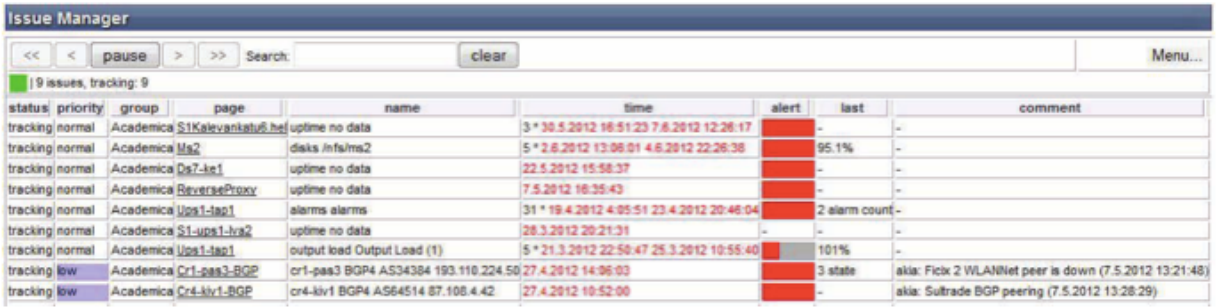


Illustration 5: Example of Issue Manager

The simplest form of root cause analysis is illustrated in the following diagram. If nodes A and B become unreachable by C, an alarm (email, SMS, issue, trap, etc.) is only raised about B being unreachable. Alarms for A are silenced. If B is configured to be under a maintenance window, it too will be silenced, and no alarms will be raised. Alarms for A will only be raised when B and C are fully operational and not in a maintenance window.

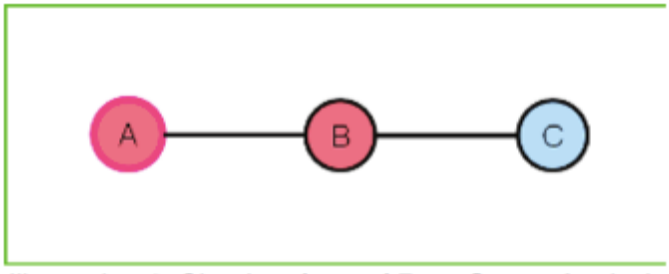


Illustration 6: Simplest form of Root Cause Analysis

Device Measurements

Traffic and Utilization Graphs

All device interfaces are, by default, measured for input and output traffic, display interface speed and utilization. Default alerts are attached to the interface utilization only, since traffic may vary between 1 Kilobit/second to 100 Gigabit/second, depending on the device, interface connection and capacity.

Reviewing a device's utilization over time can aid capacity planning or in the case of consistently low utilization reveal where there is excess capacity because of over-provisioning. Spotting over-provisioned resources allows redeployment of resources to ramp capacity where needed without additional cost.

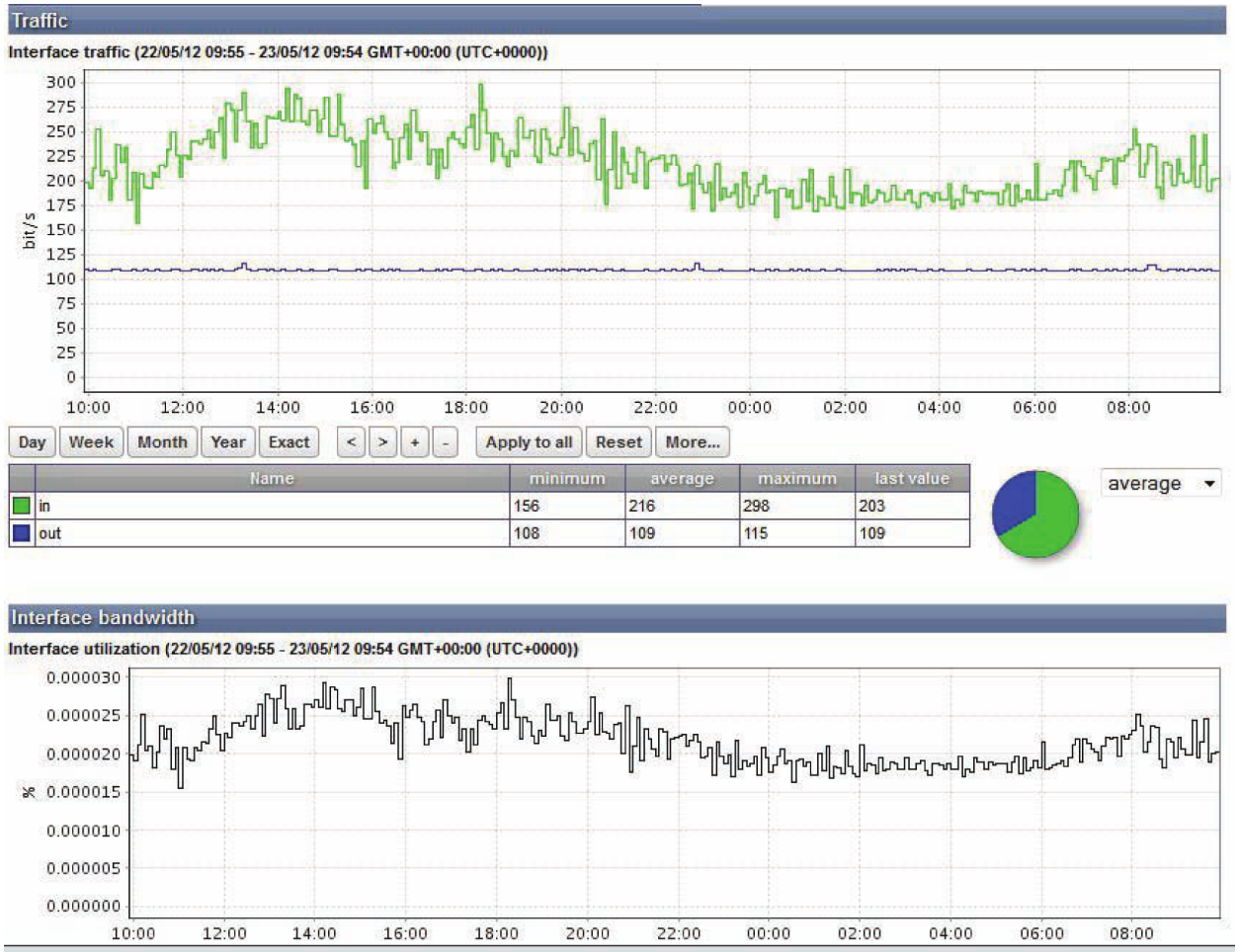


Illustration 7: Example of Interface Traffic and Utilization of a server

The graph at the top of Illustration 7 shows that the number of bits per second coming inbound vary more widely than the outbound traffic. Here this is the expected result, otherwise an alert would have been triggered. Looking at this server's historic utilization will reveal whether or not this device is over provisioned and is capable of an increased workload. Over utilization will create an alert that provides an 'early warning system' of decreased performance, for example an over utilized server will have packet loss and retransmission errors because the packets can't get access to the server. Different alert thresholds

can be configured for different disks or partitions (depending on the operating system). The disk measurements that can be collected include swap details and disk read/writes. A capacity planning report can be generated showing both high and low utilization on devices.

Server CPU Load

A single BaseN report shows the monitoring details of all the CPUs within a server - differentiating between CPUs with different colors on the graph. The details provided in the graph below assist in working out performance problems with the server's processing. For example, Illustration 8 shows an average load for most of the day around .50 but a load spike between 4 and 9 am shows a bit of a processor slow down - meaning the number of processes running in the CPU and the number of processes queued to run is higher than usual. In this case, because of the time of day it is likely a backup running.

Between 8 and 9 a.m. a load spike of 3.25 is seen. If this spike continued with a load of 3.25 we know that the processor has slowed considerably compared to the load of .50 seen for most of the day. More details would need to be investigated, such as what applications are running and how many accesses to the server are occurring, before it could be determined if there was a problem.

If other hardware measurements are available for a particular make and/or model of server, the flexibility of the BaseN service allows those additional measurements to become part of the standard data collected. The other types measurements some servers allow related to hardware problems, such as failed CPUs, damaged memory modules and faulty fans and PSU.

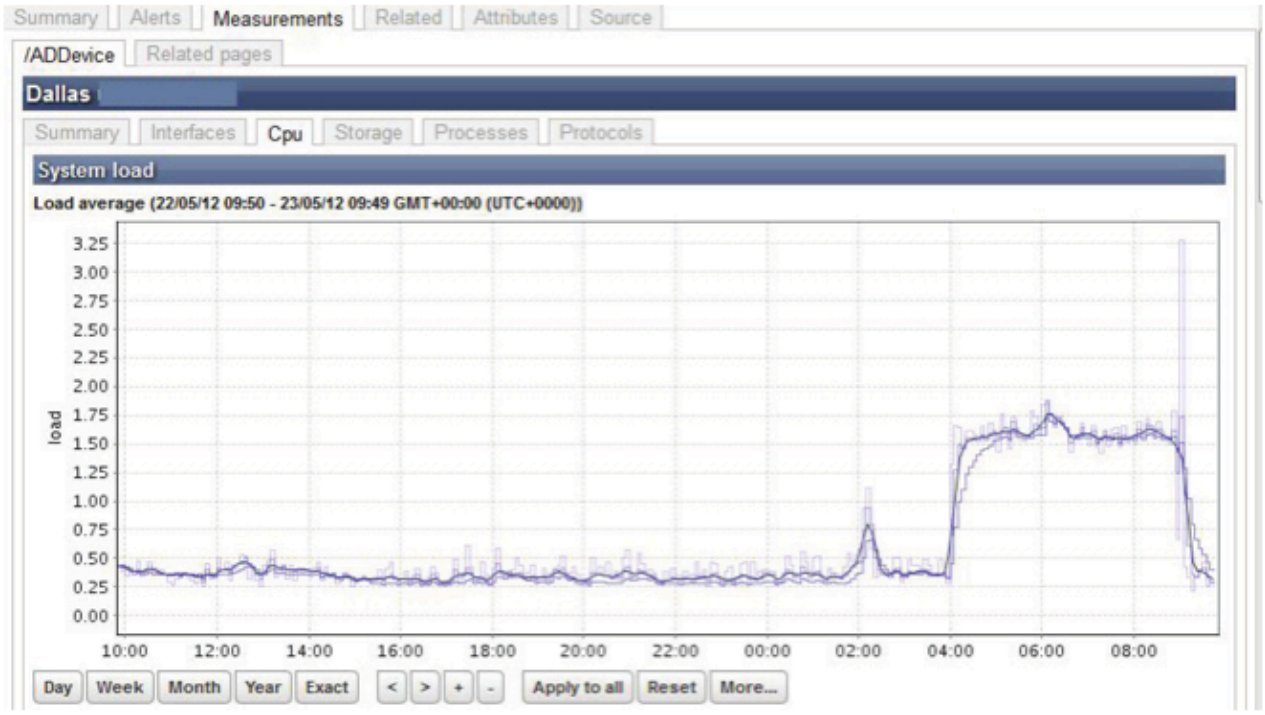


Illustration 8: Example of Server CPU Load

Memory Utilization

The memory utilization detail shown below graphs both installed physical and configured virtual memory utilization. If the server also has sway details configured, the graph can contain the sway utilization measurements, and attaches an alert if the sway utilization reaches the configured threshold value. A swap utilization alert could indicate a memory resource problem, which in turn would affect the overall performance of the device and any applications running on it.

BaseN keeps the same type of memory utilization graph and alert information for other devices such as routers and switches. When routers exceed their memory thresholds, they won't forward traffic and it is lost.

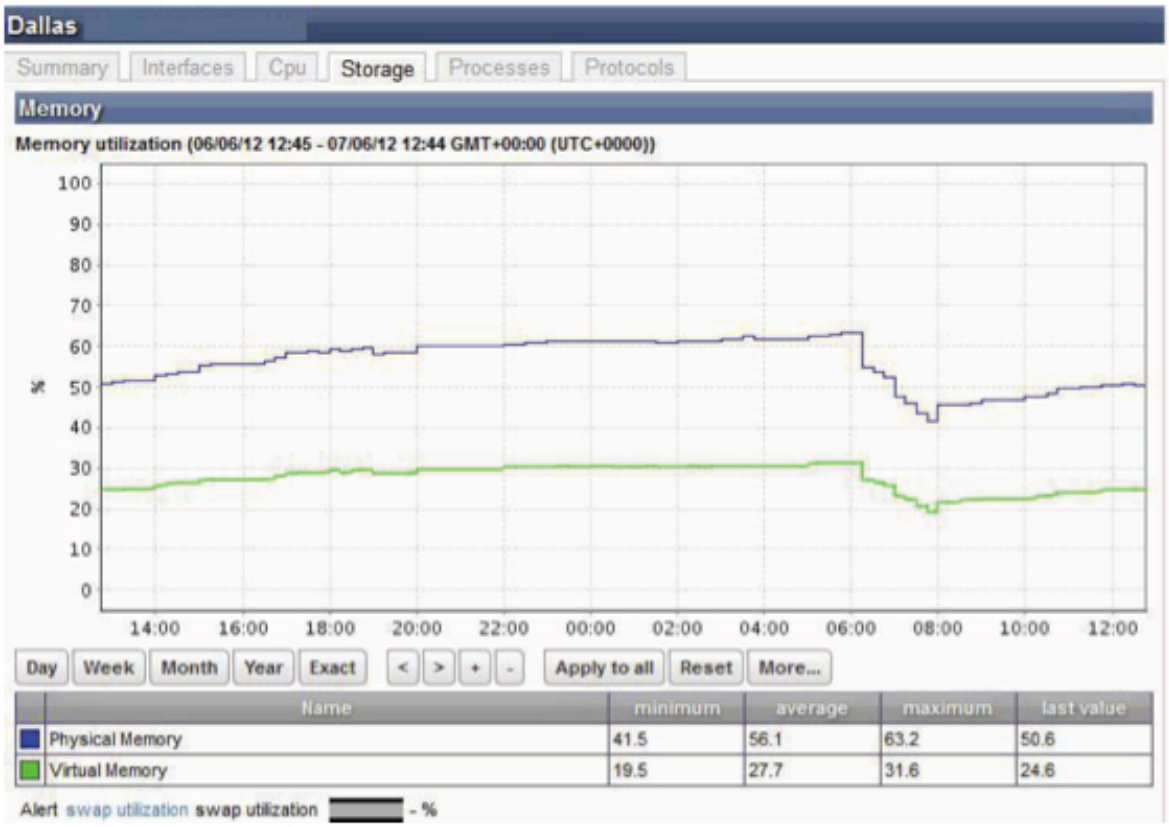


Illustration 9: Example of Memory Utilization

Application Memory Consumption

The graph below illustrates the amount of memory used by a specific application process. It also contains details regarding the amount of maximum and initial heap memory allocated to the application process by its configuration. Modifications of the configuration of allocated process memory will be visible in this graph.

Illustration 10 relates to a Java process, where the heap memory is used to store Java objects. The BaseN Java measurement templates also include a similar graph for displaying utilization of Java non-heap memory, which is used for storing loaded Java classes.

Different types of applications would, in the BaseN Template Library, have other or different memory configuration and utilization measurements available.

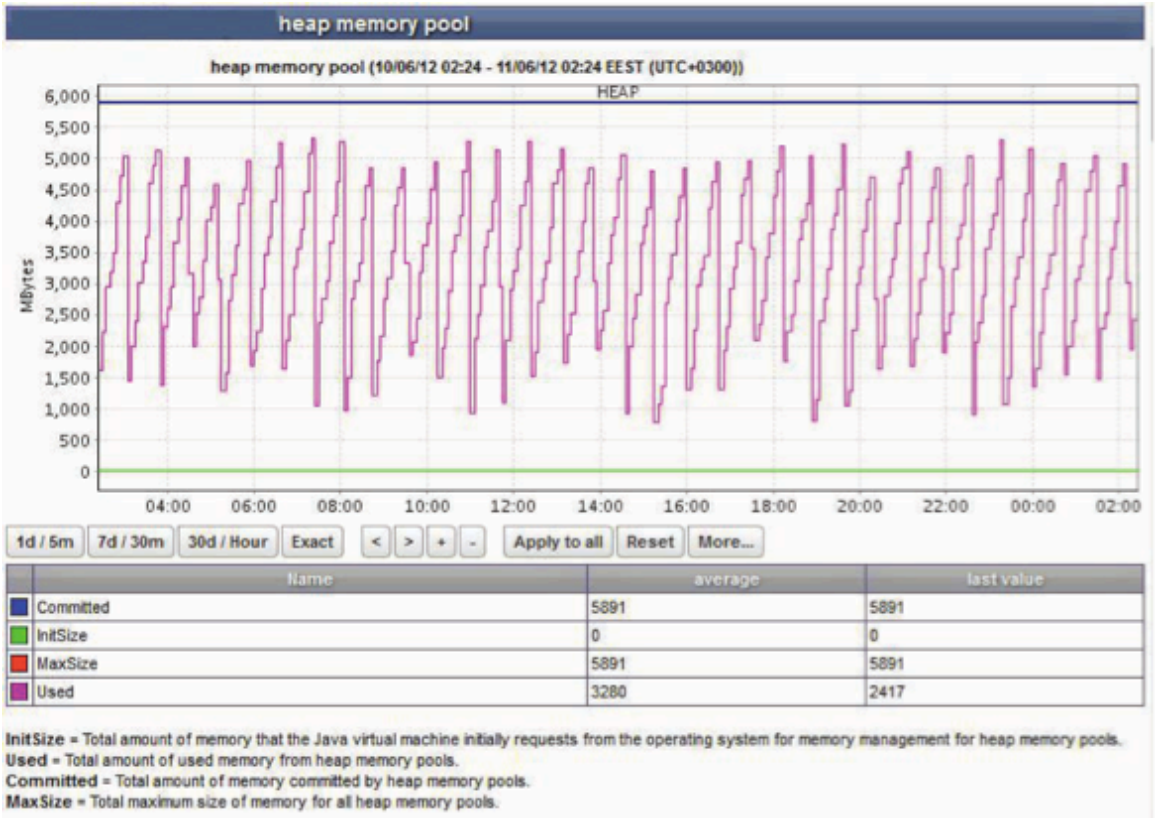
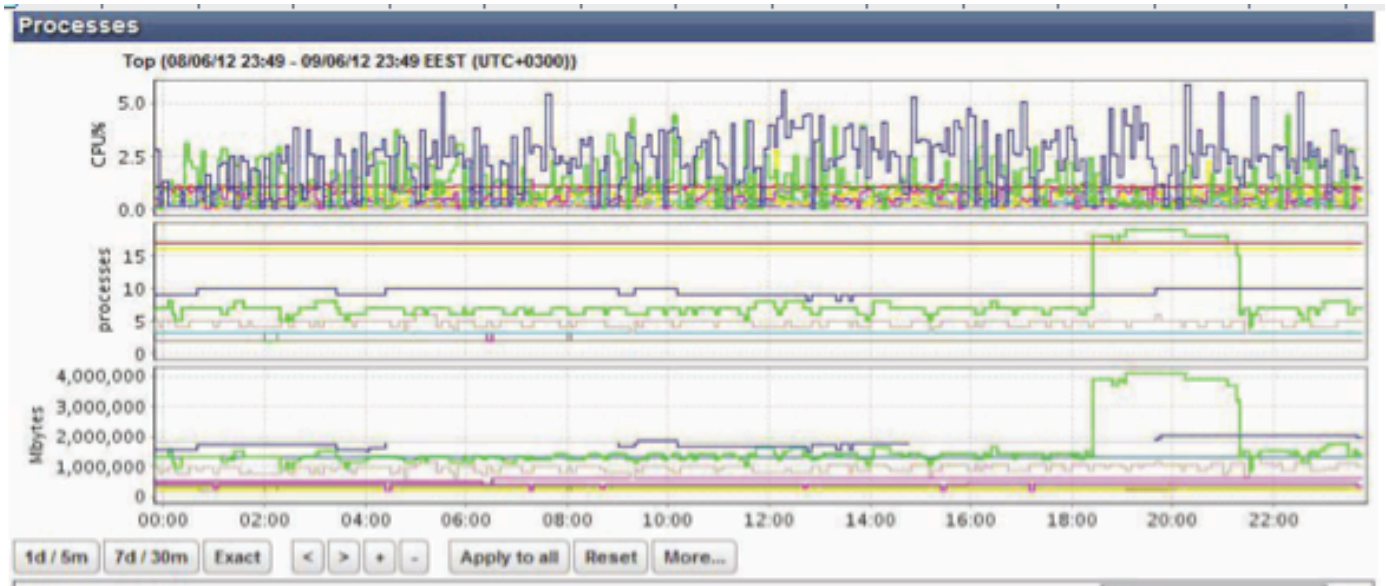


Illustration 10: Java Heap Memory Pool

Device Processes: Memory Leak

This graph contains, by default, the top 30 processes, based on CPU utilization, of the device. The measurement can be configured to display a customer specified number of processes which could assist with troubleshooting performance problems of applications.

Illustration 11 indicates if a process is using unexpected amounts of memory and CPU. Processes use and release CPU and memory in their normal operation. If a process takes memory but doesn't release it when through it is said to be leaking memory. Memory leaking will eventually create a CPU or memory utilization alert or create a fault and require a device reboot. If any application, such das Java, leaks memory, eventually there will be no memory available for other processes to run. Monitoring Java and other top processes running on a device provides a warning that memory leakage is happening before an actual problem occurs. This gives the network operator the opportunity to avoid downtime of the device and enables zeroing in on the problematic process.



43 rows displayed — Filter... clear

Name	minimum CPU%	average CPU%	maximum CPU%	last value CPU%	minimum processes	average processes	maximum processes	last value processes	minimum Mbytes	average Mbytes	maximum Mbytes	last value Mbytes
snmptablesnitch	0	2.29	5.82	1.46	8	9.5	10	10	1368073	1810126	2055990	1961075
webformsnitch.p	0	1.28	4.39	1.47	4	8.18	19	7	877161	1677928	4089232	1439564
logcopier.pl	1	1.08	1.17	1.07	1	1	1	1	0	0	0	0
dnssnitch.pl	0	0.65	1.39	0.903	1	1.98	2	2	194446	404777	441674	332310
agent2.pl	0.187	0.617	2.95	0.535	16	16	16	16	0	0	0	0
tcpsnitch.pl	0	0.569	0.89	0.354	1	1.02	2	1	188237	208643	432189	221742
java	0.283	0.388	0.535	0.453	3	3	3	3	0	0	0	0
websnitch.pl	0	0.331	0.741	0.158	3	4.66	6	5	587267	947716	1315121	998733
dsm_sa_snmp32d	0.158	0.193	0.225	0.187	1	1	1	1	3.76	3.76	3.76	3.76
autodiscover.pl	0	0.117	0.744	0	1	1	1	1	0	0	0	0
snmpd	0.0166	0.0337	0.0501	0.0333	1	1	1	1	324575	324575	324575	324575

Illustration 11: Example of Process table

Application Servers

Illustration 12 shows the number of sessions which are active on a type of Load Balancer. The large variation in the usage of the virtual servers may indicate that a number of the virtual servers are unused and could be redeployed.

Illustration 13 shows the session details expressed as number of sessions/second.

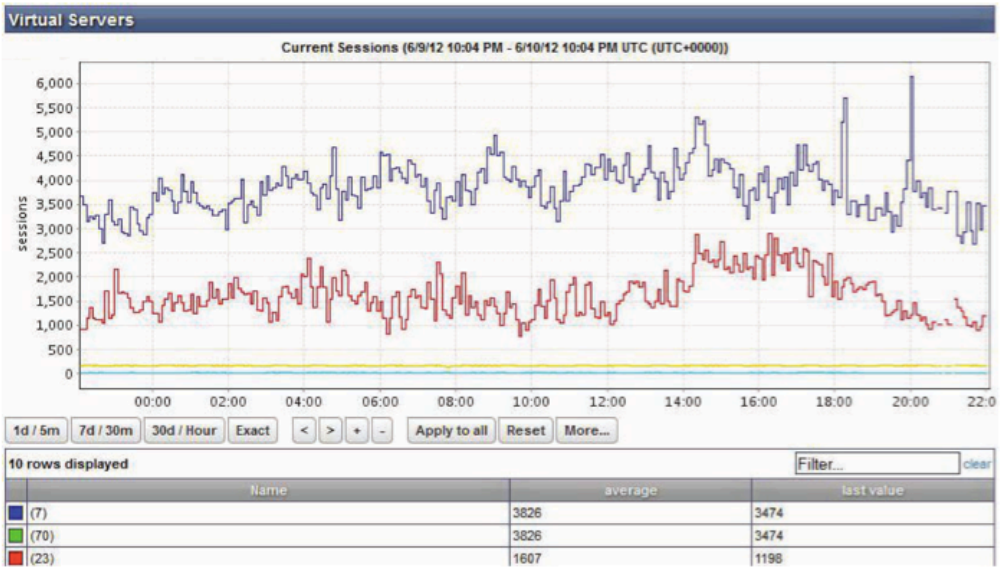


Illustration 12: Current Session of Virtual Servers

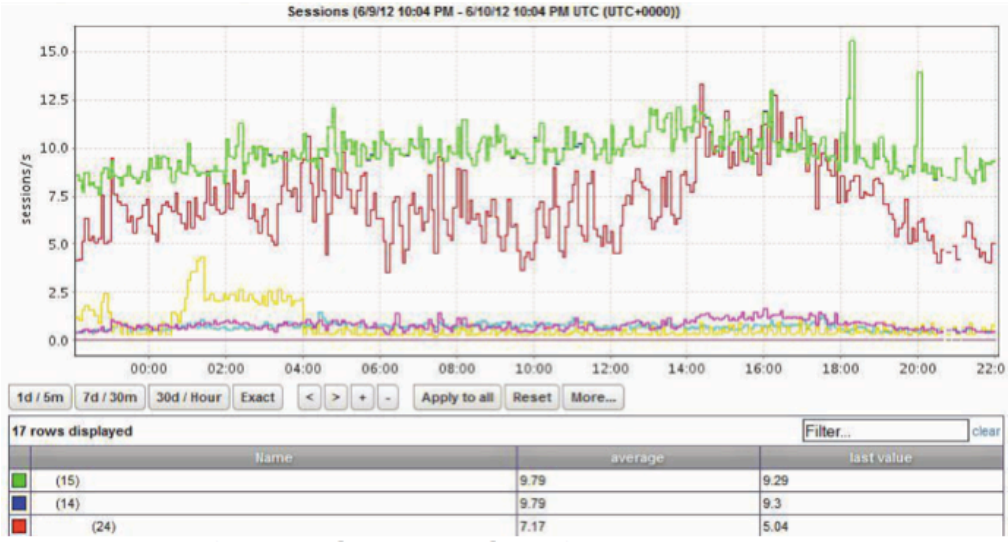


Illustration 13: Load Balancer Sessions per Second

Quality of Service Monitoring

This graph illustrates Quality of Service (QoS) measurements in a network, indicating the real time performance that a user experiences. It shows how much and how fast traffic flows on this circuit throughout the course of a day, providing insight into the user experience. Except for a few peaks, traffic in the Bronze category is flowing at about 55 kbits per second. If network personnel want to see more detail about the peaks, they can highlight the time span of interest and traffic flow can be seen down to the minute level. The BaseN service also measures dropped traffic as a QoS parameter.

Service level monitoring is another category of BaseN QoS monitoring. In addition to graphic reporting of SLA service, alert thresholds can also be set. The BaseN service can also look at what SLA percentages have been experienced and make estimations of what the SLA will be.

One BaseN user provides network and computing services to 2000 stores. Depending on the size of the store, different SLA requirements are contracted. The BaseN service enables each store owner to have a portal to view the service levels their store experiences. When clerks feel that the devices have slowed down, they can verify it on their BaseN portal and call tech support before network services completely degrade of fail.

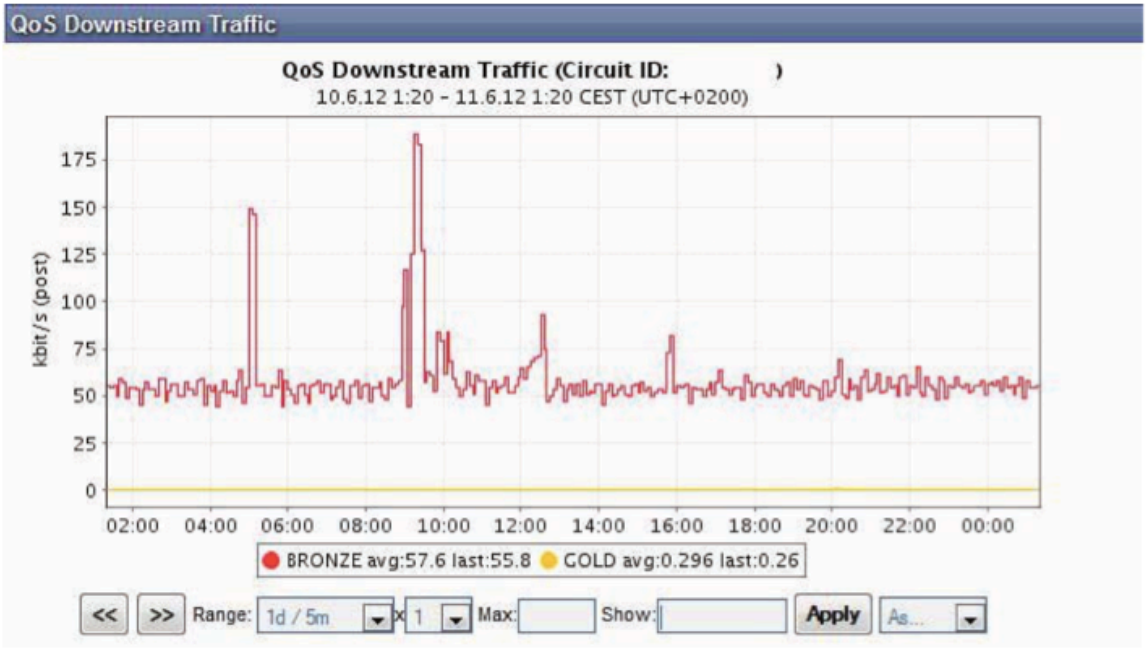


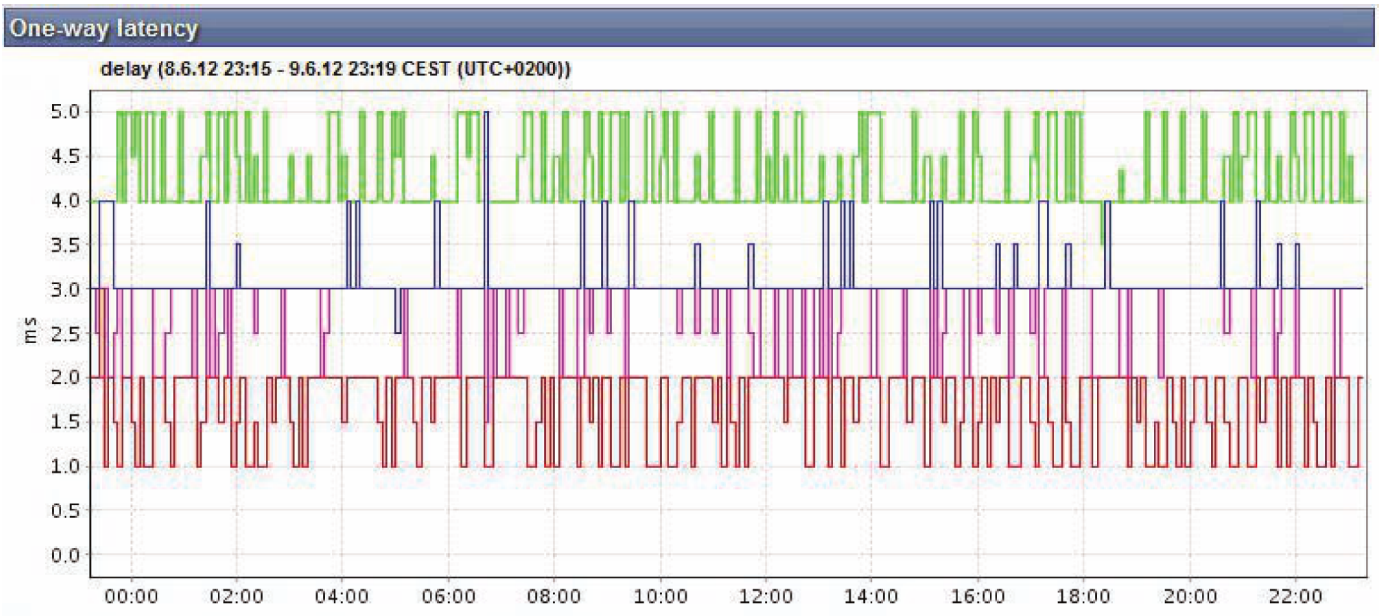
Illustration 14: QoS Downstream Traffic

VoIP Quality Management

One-way latency measures the time it takes a packet to travel in one direction and is measured in ms. If latency is too long, the quality of the voice over IP service experiences delay, which may degrade quality or create echo.

Illustration 15 below shows measurements of One-way Latency, Destination to Source (DS) and Source to Destination (SD) between two devices. This particular BaseN template is using the CiscoSAA feature to configure and measure latency, jitter and packet loss. Mean Opinion Score (MOS) data can also be graphed based on the collected values as shown in Illustration 16 on the next page. The MOS value is a commonly used indicator for VoIP quality.

Illustration 17 graphs jitter in relationship to the average Round Trip Time (RTT). If jitter, the time latency between packets in a given transmission, has too great a deviation when compared to other transmissions this will contribute to the degradation of service, as either a delay or echo, even if the average RTT has not degraded.



11 rows displayed

Filter... clear

Name	last value
AvgDS	2.56
AvgSD	3.75
MaxDS	3
MaxSD	4
MinDS	2
MinSD	3
NumOfOW	1500
Sum2DS	10170
Sum2SD	21410
SumDS	3834
SumSD	5630

Illustration 15: One Way Latency

VoIP QoS Monitoring

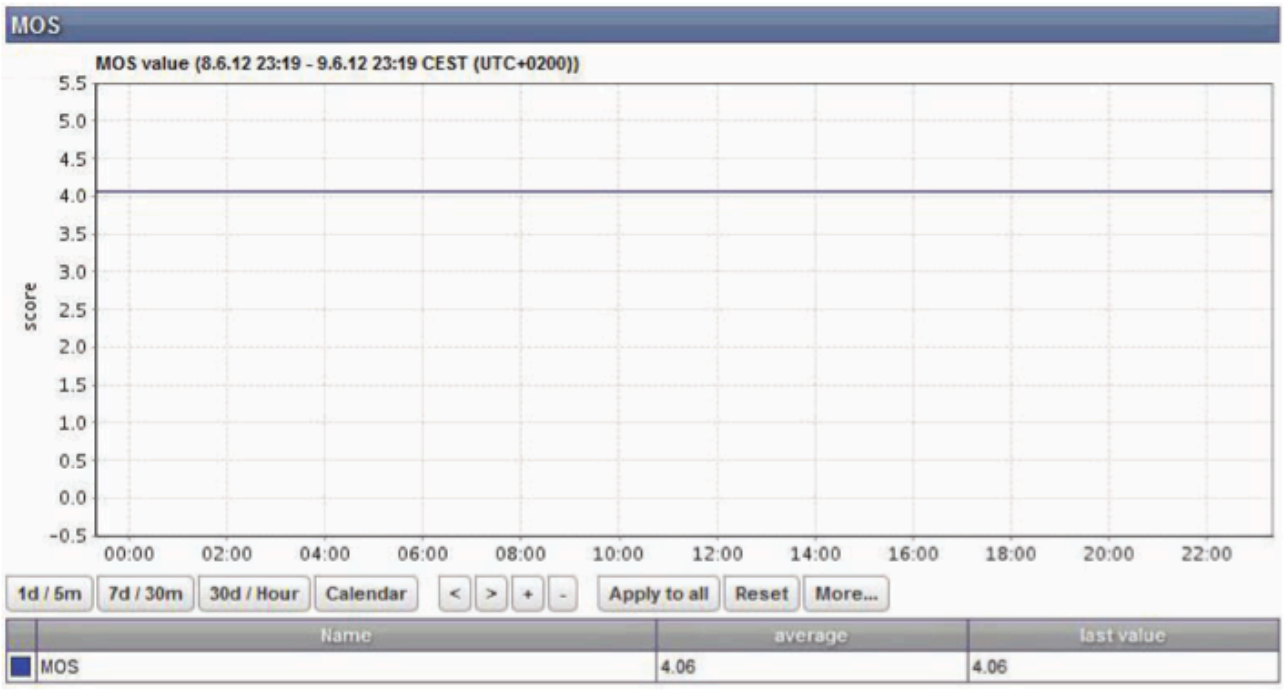


Illustration 16: Mean Opinion Score – MOS

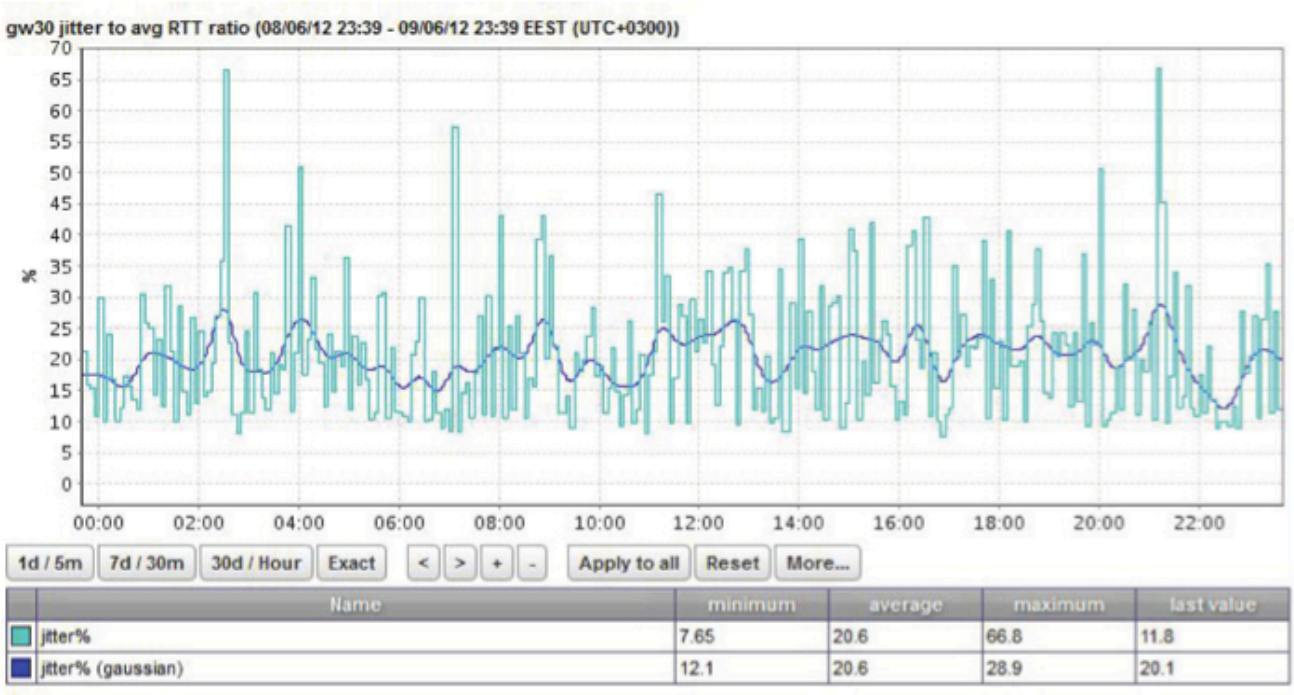


Illustration 17: Jitter on Average Round Trip TimeRatio

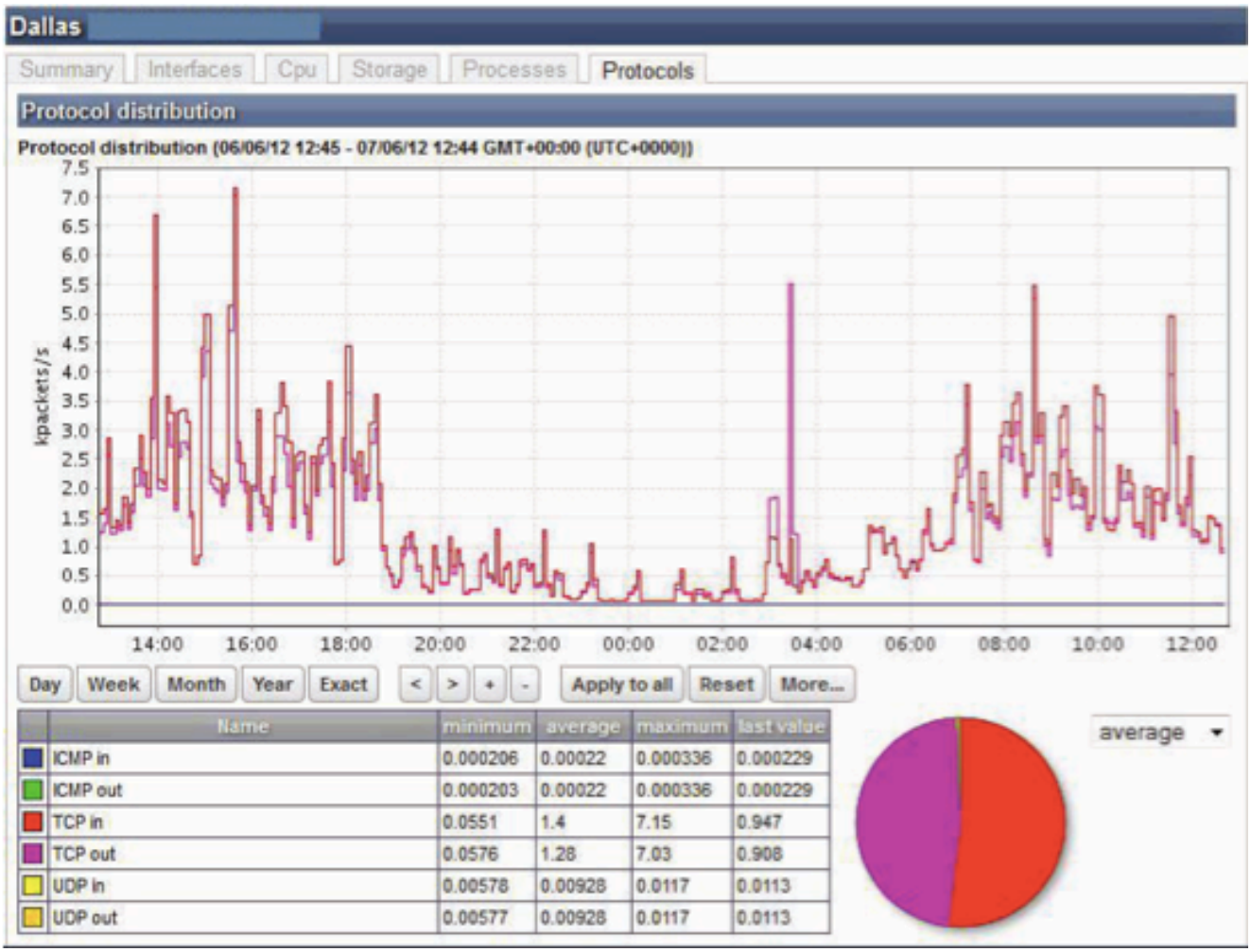
VoIP Peer Measurements

The graph below shows a monthly view of the numbers of calls per second registered on a VoIP peer/gateway. This particular example is showing the highest number of calls to the Plain Old Telephone System (POTS) service of the VoIP peer. This may be an indication for this user to enforce VoIP calling for internal use as a cost reduction measure.

Illustration 18: VoIP Success Calls

Protocol Distribution

There are several protocol performance measurements related to the type of traffic on the device. The first provides a breakdown of the main protocols used on a device, and splits into input and output traffic. A sudden or unexpected change in the protocol distribution may indicate a problem or Denial of Service (DoS) or Distributed Denial of Service (DdoS) attack.



Name	minimum	average	maximum	last value
ICMP in	0.000206	0.00022	0.000336	0.000229
ICMP out	0.000203	0.00022	0.000336	0.000229
TCP in	0.0551	1.4	7.15	0.947
TCP out	0.0576	1.28	7.03	0.908
UDP in	0.00578	0.00928	0.0117	0.0113
UDP out	0.00577	0.00928	0.0117	0.0113

Illustration 19: Example of Protocol Distribution

TCP Sessions

The information contained in Illustration 20 is useful in troubleshooting performance related problems. It shows the number of established sessions to this server over a 24-hour period. A daily pattern will be created over time that will provide a visual cue when abnormal circumstances occur. BaseN can also alert on the number of established sessions - too few or too many sessions is an alert condition. Alerts on this condition must be set based on how the server is being used and so must be set by customer.

If the established threshold for Illustration 20 is a 450 sessions maximum, then an alert condition is created around 15:30 in the afternoon the threshold is exceeded. The alert is reported to the IssueManager and shows on the real time LocationMap and device alert screens as well. A high sessions alert will lead a network operator to watch if connections to the server are denied, thereby effecting an end-user's performance. If no sessions are being denied, then end-users are unaffected, but the network operator has the early warning and can continue to investigate what is causing the unexcited results. This creates an opportunity to repair the situation before a complete failure occurs.

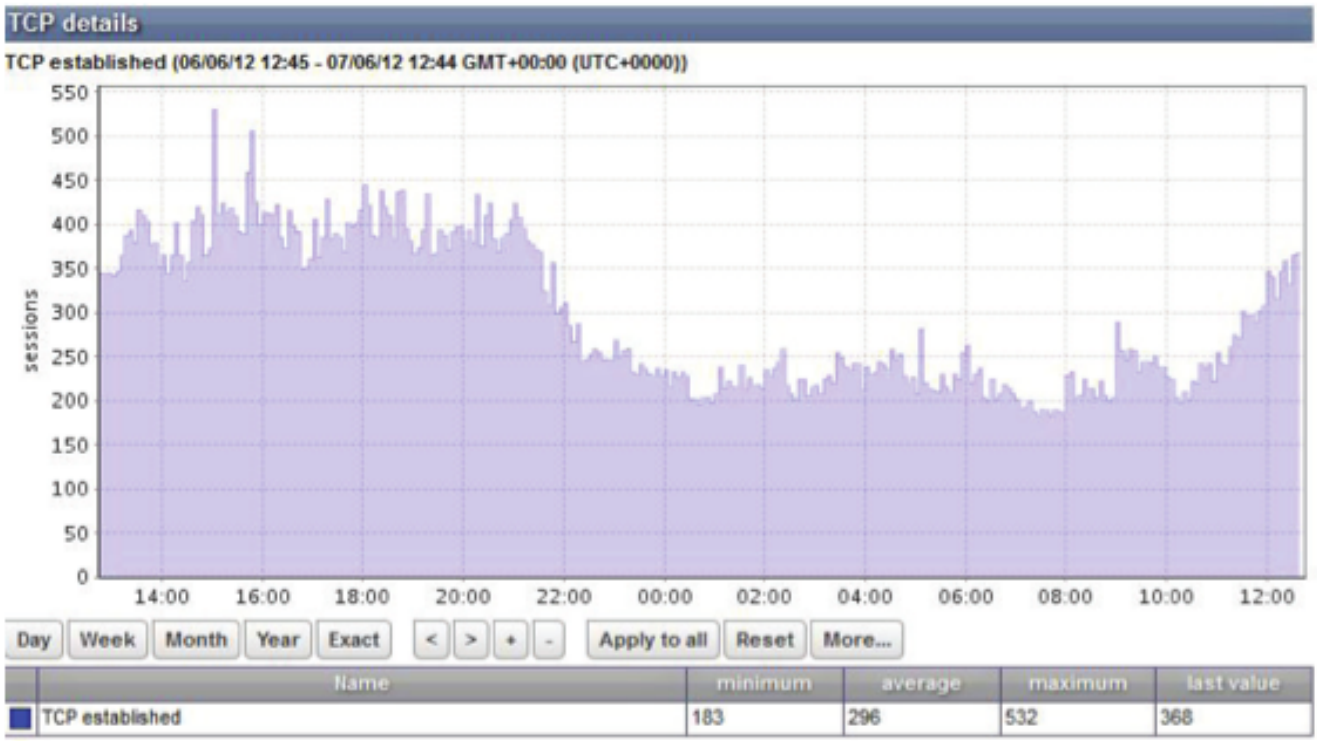


Illustration 20: Number of TCP Sessions

TCP Protocol Details

The graph below provides further details for all the TCP sessions listed in the previous measurement. The information would help indicate if the device is having problems or connection issues. The desired condition is no TCP errors and very small values for resets and attempts failed. Illustration 21 shows several retransmissions at 18:00. Highlighting over the time period in question will break it down into smaller time segments, so that a minute-by-minute view can be gotten for the 5 minute window before and after 6 p.m. which could provide insight into the problem. This 10 minute period can also be reviewed in the IssueManager for alert conditions that caused the retransmissions.

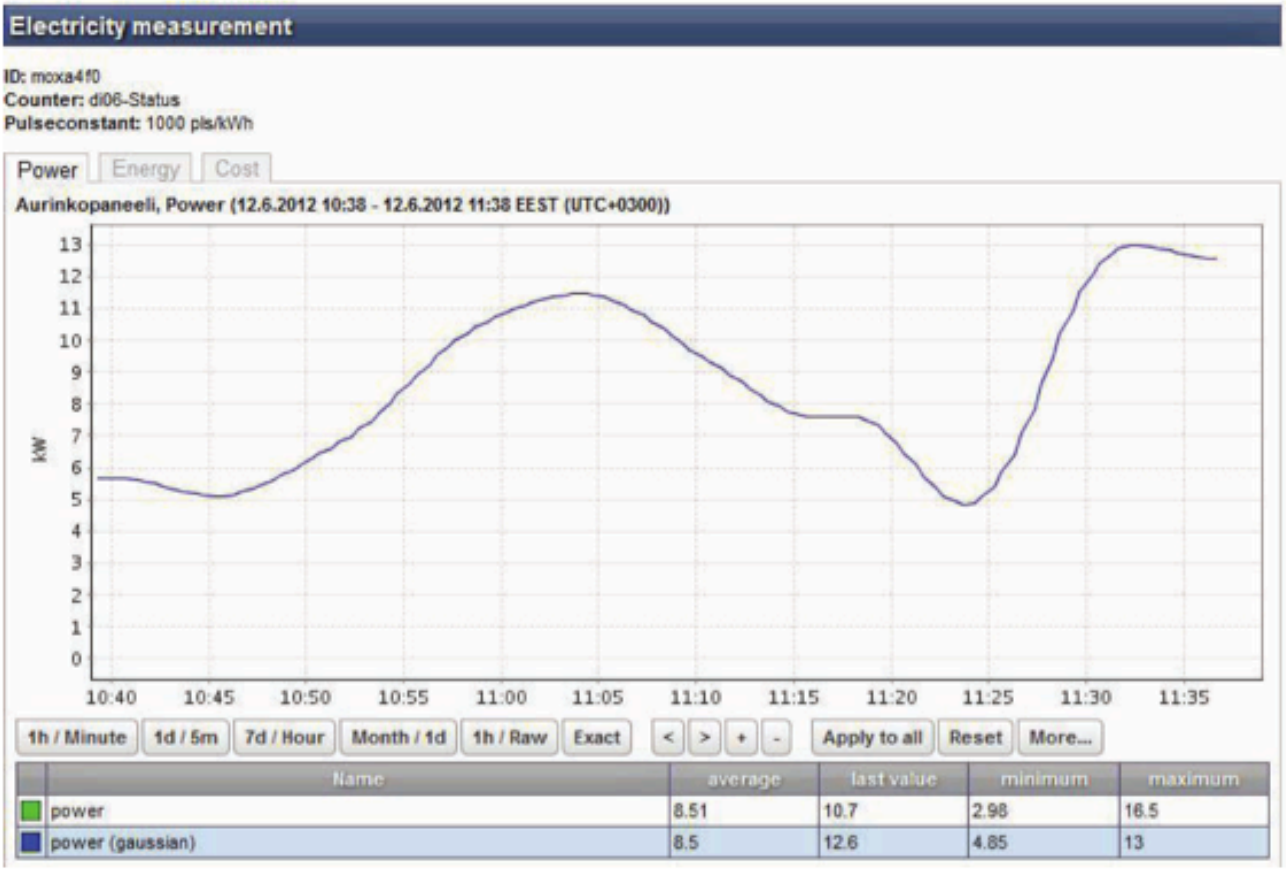


Illustration 21: TCP Protocol Details

BaseN Can Monitor All Types of Devices

BaseN can collect measurement data and status information actively (SNMP or other means) or passively via Syslog messages, SNMP traps, or email reception.

We can monitor smart meters, home energy devices, credit card readers, solar panels and mobile radio/base stations. As well as any other device from which we can collect data.

After IP and ICT, smart grid and home energy monitoring is our next largest market sector. The next 3 graphs illustrate the type of energy monitoring BaseN can do. For more information about BaseN energy monitoring, please see the BaseN Service Description for Smart Grid and Energy Consumption Monitoring.

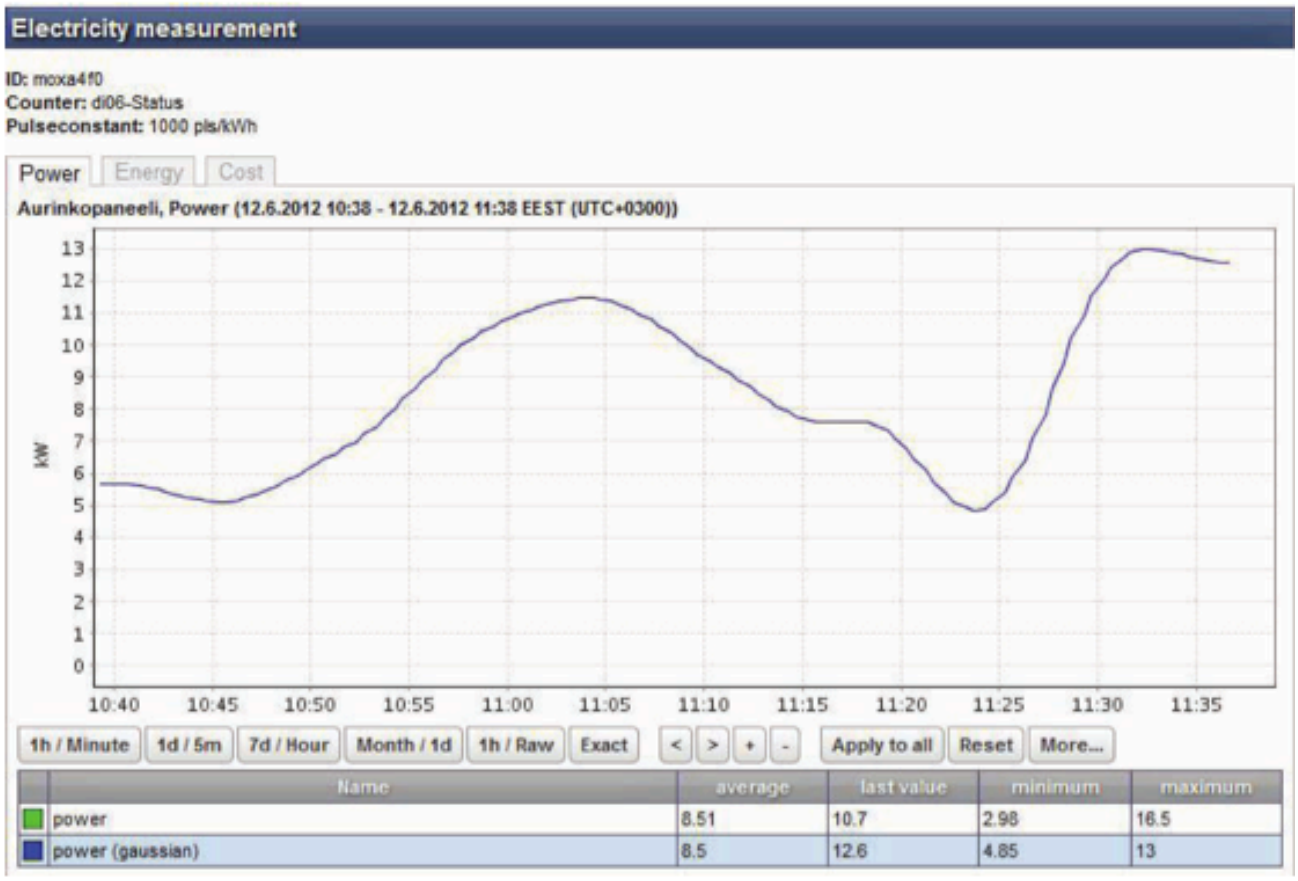


Illustration 22: Power Generated by a Solar Panel

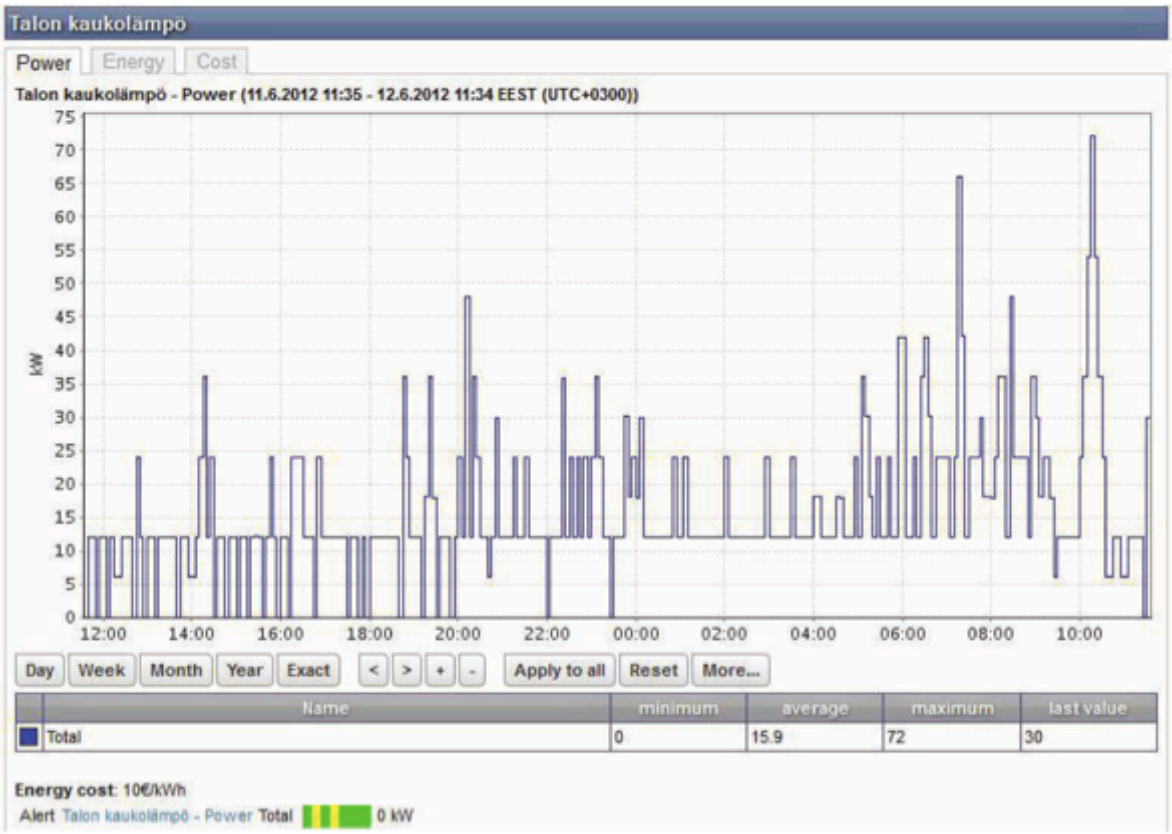


Illustration 23: Building Heating System Consumption per kWh

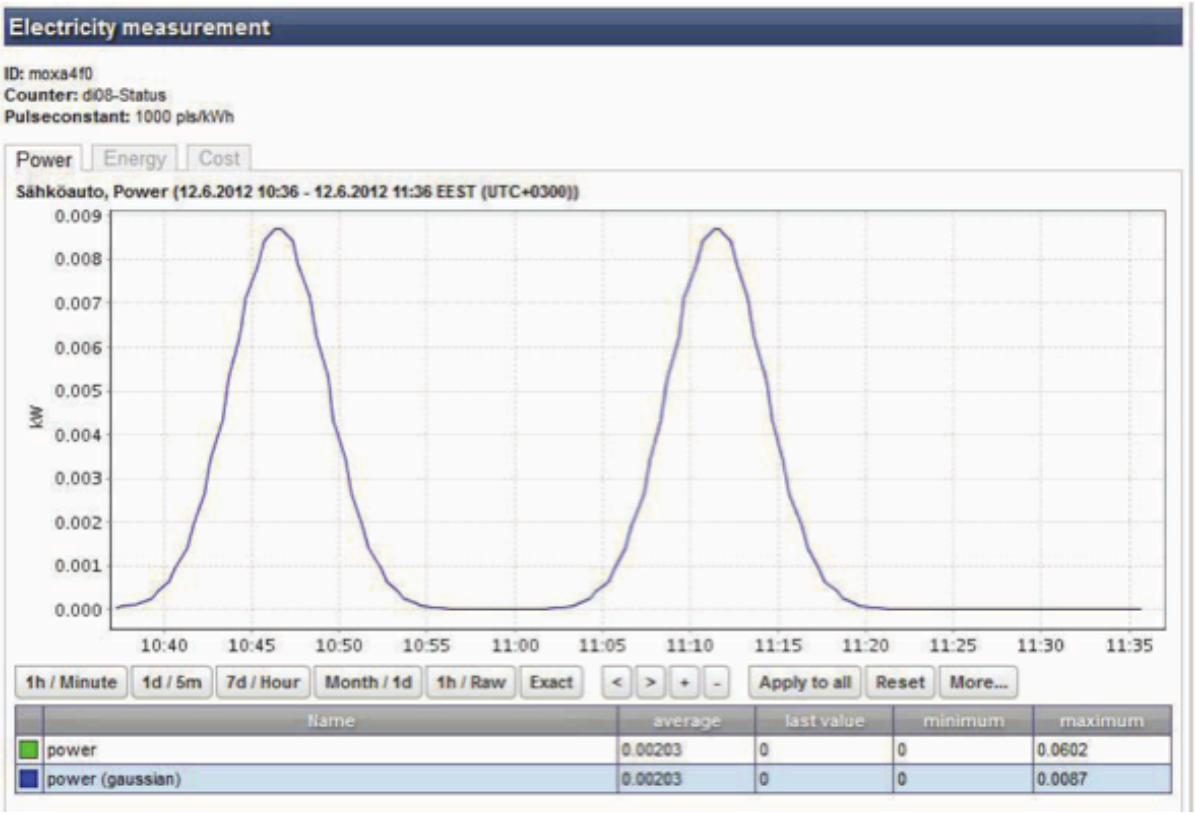


Illustration 24: Power Utilization for 1 Apartment Over 2 Hour Period

Portals for Users and Their Customers to View the BaseN Service

Export and Web Services

Data export and web services access make viewing all BaseN data easy wherever you are. Alerts can be sent to NOC operators via SMS and email to ensure the fastest response to the most critical problems. Daily, weekly or monthly reports can be automatically generated as XLS or PDF files and sent via email, or saved as an attachment in the portal. Measurement details can be exported to PDF and XL formats to create customized reports. Graphs can be saved as PDF, XLS, CSV and Image (PNG and JSON) formats. HTTPS and BABUP can be used to export alert details and measurements, generally in XLS and CSV formats. Scripted export/output formats can be any format within Java script capabilities.

Web Services and End-user Portals

The Web Servers make all of BaseN's real time data, alerting information, graphics and reports available on an IP network. You can access your own BaseN Service portal through a PC, iPad or mobile device with web browsing capability. End-users can have authorization to different levels of information. The ability to interact with real time alert information will likely only be authorized NOC personnel. A capacity planning manager may want access to only utilization graphs and reports. This allows for high availability, flexibility and practicality in field conditions and in delivering relevant content throughout the organization.

There are multiple web servers within the BaseN service cloud to ensure a high availability in the event of outage or equipment failure. The grid architecture makes the BaseN Platform well suited for simultaneous access multi-user applications. If more capacity is required, more web front-end servers can be added to the grid. If desired, the web access capability can be FIPS 140-2 certified, and it can have a two factor authentication process.

Portals for Your Customers

Many BaseN users provide services to their own customers and give them BaseN portals to view the performance and faults of the provided service. The Customer Portal is used to allow read access to a subset of BaseN Platform pages. These pages are designed to meet the needs of the individual customer. BaseN users can have dedicated portals for each of their customers. No customer can access another's data.

The flexibility of the BaseN services enables portals to be customized. Some users put their own name, logo and GUI on their customer portals. Portal access, appearance and display is customizable with logos, pictures, colors, and style sheets. A portal begins with a login screen and can include performance and SLA reports, on-line help and contact information.

More BaseN Function Details

Device Templates

Device templates are at the heart of the BaseN service. Currently there are over 1800 templates in the library. The templates are easy to work with and can be amended to include specific monitoring or reporting capabilities that a user desires. New templates are being written all the time. Templates can take a few hours or several weeks to create, depending on their complexity. With BaseN you'll never have to wait for a general software release to monitor a new device or service. All templates are hot deploy-able, meaning that the system doesn't have to be rebooted to activate the new device template - it is added to the BaseN service and begins monitoring.

All templates are stored in BaseN's template library. If you have questions about whether or not specific devices are already monitored, you can ask your BaseN Account Manager. Because BaseN adds templates almost weekly it is impossible to have an up-to-date list anywhere but the template library.

Auto Discovery and Inventory Management

The AutoDiscovery function allows the BaseN service to detect devices and automatically begin collecting measurements and monitoring details. AutoDiscovery information can be entered as one or several host addresses, or larger network ranges.

This function can also help with inventory management as the configuration details the BaseN service detects will help verify what equipment is located where. The information collected can also be uploaded into Excel or as an XML file from a CRM system.

On request the BaseN service can also be customized to collect configuration data from your user systems or databases.

Alert Details

Alerts can be silenced either by configuration of one or more Alert Time Lists (ATL) which specifies recurring days or time of day when an alert should be silenced for routine maintenance. ATLs can specify that alerts are silenced on weekends, during the night, or on holidays. For unscheduled maintenance alerts can be silenced using the Maintenance window.

The BaseN Platform contains default alert dependencies which are based on our experience and some assumptions of service technology. At times the default dependencies may have to be adjusted according to user requirements or local service topology which our service can not always discover with our automated tools.

Users can adjust various settings for an alert by using the Alert Modify function. Adjustments that can be made to an alert include: adjusting threshold values, priority, and escalation of the alert. The escalation of an alert will change the fixed status bar to a status bar which flickers to increase visibility. Alert modification, like silencing, priority and escalation would also allow for adjustment of alert dependency where required.

Configuration of alert categories enables the creation of a dynamic overview of all alerts placed in their configured category. A selection of icons available to depict the most commonly used categories.

The Alert - Add to Cart function may be used to place a selection of alerts in a separate ‘cart* which would enable a user to keep the particular alert selection in a collected view. The collected view can be a mix of alerts from various devices, services, networks or other entities - any combination of alerts that are meaningful to the user can be collected into one view.

The BaseN service is scalable, nimble, resilient and cost-efficient. BaseN’s pay as you go model lets you buy the service you need now, and easily expand as your network grows. New devices in your network are never going to be a problem with our extensive template library, and our ability to create and deploy new templates as needed. Talk with your BaseN account manager and let him assist you in choosing the BaseN service solution that is most useful to your organization.