02-03-2020

CNaaS Service Definition Template/Checklist

Work Package	WP6
Task Item:	Task 33
Dissemination Level:	PU (Public)
Lead Partner:	UoB/AMRES
Document ID:	GN4-3-20-23795cf

Authors:	Maria Isabel Gandia (CSUC/RedIRIS), Ivana Golub (PSNC), Susanne Naegele-Jackson (FAU/DFN), Pavle Vuletić (UoB/AMRES), Tim Chown (Jisc), Jasone Astorga (RedIRIS/University of the Basque Contry), Vidar Faltinsen (Uninett), Asko Hakala (Funet), David Heed (SUNET))

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

Abstract

This document is a service definition template that can be edited and adapted by anyone who wants to offer campus network management as a service to their end-institutions, and to produce their own service definition and contract documents. Relevant topics to consider when writing a document based on the template are also included.

Table of Contents

1 CNaaS Service Definition Template/Checklist

1.1 CNaaS Service Definition

As the Campus Network Management as a Service (CNaaS) service can be offered in different ways, the National Research and Education Network (NREN), regional network or institution offering CNaaS services (the ‘provider’) and the end-institution (the ‘customer’) must agree on the exact definition and scope of the service:

- What is included in the basic package of the service.
- What is added in an extended or supported package.
- Define any demarcation points between the provider and the customer.

It is very important to define and agree all details before going into production. The provider and customer can sign a contract or Service Level Agreement (SLA) that will contain the particular aspects they have agreed for the CNaaS service,e.g. quality, availability, responsibilities.

The following sections provide a service definition, based on ITILv3[1] processes and functions [ITILv3], that is easy to adapt and replicate. It can also be used as a reference when writing the contract or Service Level Agreement. When writing their own Service Definition Document, the provider can modify the text to fit their needs and adapt the examples. It is up to the provider to include as many technical details as desired, although where many details are given, they are more likely to change in the future. The provider should reserve the right to change the architecture, software, configuration mechanisms or monitoring infrastructure according to the needs of the service, the evolution of the technology, the tools and the network.

[1] A new version of ITIL, [ITILv4], appeared by the end of 2019, although not all the books were released by the time of writing this document. According to AXELOS [AXELOS], ITILv4 does not invalidate earlier versions of ITIL, therefore the ITIL v3 approach is still valid.

1.2 Terminology

There are several important terms for the CNaaS Service Definition, whose meaning, as used in this document, is provided below:

- **Provider** -The organisation that is providing the CNaaS service (NREN, Regional network, institution or service provider).

- **Customer** - The end-institution contracting the CNaaS service (University campus, school or any other organisation that plans to outsource the network monitoring, network configuration and management or some of its functions).

- **Supported Service Package** – A set of activities, that form a service that the provider offers to the customer as a part of the CNaaS service. One or more service packages can be offered by the provider and contractually agreed between the provider and the customer.

- **Supported Network Items and Services** - Network items and services that are covered by the contract.

- **Additional Network services** - Services that are related to the network but not specifically a part of the wired or wireless network. Some examples would be DHCP, DNS, VPN, RADIUS, LDAP, NTP, VoIP or any other network-related services that must be agreed upon beforehand between the provider and the customer.

- **Network Management and Monitoring System** – A system used by network administrators to manage the network components and constantly observe and measure parameters to check the health of the network (software, hardware and environmental parameters) and for notifying the network administrator in case of trouble.

1.3 Contacts/Roles

The contact details of all roles must be exchanged between the provider and the customer, and updated promptly if they change. More than one person can be associated with a role. Likewise, depending on the case, more than one role can be assigned to a single person.

The provider should define a person or a group for each one of their defined roles. Some suggested roles are:

- **Product Manager**: the main person responsible for continuously developing and managing the CNaaS service as a whole and for handling its commercial aspects.

- **Service Manager**: a person that will follow all the stages of the CNaaS service and liaise between the customer and the CNaaS team at the provider. This person will also try to resolve any complaints received about the service and effect any adjustments or further development that may be needed, referring to the Product Manager or the DevOps team if necessary.

- **Technical Advisor**: a person that provides technical knowledge and advice to support the customer during the design and transition stages.

- **NOC Team**: Network Operation Centre that assists the customer during the operation stage, providing 2nd (and depending on the agreement, 3rd) level support.

The customer should define a person or a group for each one of their defined roles. Some suggested roles are:

- **Service Coordinator**: the customer’s main point of contact with the provider will be the main person responsible for continuously following the evolution of the service, attending meetings, asking for incident reports, suggesting service improvements and passing on any complaints to the provider.

- **Helpdesk Team**: the team responsible for supporting end users in using the CNaaS service on site and providing the main point of contact in case of any issues.

During the service design stage, at least the Service Manager, the Technical Advisor and the Service Coordinator should meet face-to-face and exchange information to define the exact scope, involved packages, architecture, expected timeline, SLAs and any other relevant parameters to define the service.

If necessary, the provider and the customer can also specify some roles to be used for the transition stage of the CNaaS service and for any change management required during the service’s lifecycle. For instance:

- The members of the Change Advisory Board (CAB), responsible for oversight of all changes in the production environment.

- The members of the Emergency Change Advisory Board (ECAB), responsible for oversight of all emergency changes in the production environment (for example, to resolve a major incident or implement a security patch).

1.4 Service Delivery Model

As the CNaaS service will be offered by each provider to their customers, the Service Delivery may differ from one provider to another. Therefore, the provider and the customer must agree on the offered packages, related parameters and prices, if applicable, before offering the service. The next sections suggest possible supported packages as well as service elements to be agreed beforehand for each customer and service package.

1.4.1 Supported Service Packages

The service can be offered in separated standardised packages by the provider. A basic package can be defined with the minimum requirements and offerings of a CNaaS service (for example, monitoring of the infrastructure). Subsequent packages (like configuration and management of the wired/wireless network or additional services) can be added to the basic package, depending on the customer’s needs and the provider’s offerings. The following subsections suggest some packages that the provider can offer to the customer, although each provider can define different service packages to their customers.

1.4.1.1 *Monitoring of the Infrastructure*

The monitoring scope should be defined and the level of detail given in the Service Definition may vary depending on the case. For instance, it may indicate that the provider will install all the necessary software tools for the correct monitoring of the infrastructure, without listing the specific software tools.

The following list shows examples of items that can be included in the Service Definition. The same list can be used as a reference for the monitoring of additional services:

- What will be monitored (included pieces of equipment):
  - Routers
  - Switches
  - Firewalls
  - Access-points
  - Network links
  - Intrusion Detection Systems
  - Radio links

- What will the monitoring system do:
  - Trigger alarms when defined thresholds are reached (send to the Campus HelpDesk/the NOC/an alarm console, etc.).
  - Generate graphs (Daily/Weekly/Monthly/Yearly, on-demand, etc.).
  - Automatically generate tickets when defined thresholds are reached (supported platforms).
  - Monitor certain Key Performance Indicators agreed with the customer.
  - Generate automatic reports.
  - Store monitoring data.

- Parameters to be monitored:
  - CPU usage
  - Memory usage
  - Interface input/output traffic
  - Interface input/output errors
  - Tx/Rx optical power (where possible)
  - Specific log entries like up/down interfaces
  - General availability
  - Latency in pre-defined links
  - Module up/down (for chassis based or stacked equipment)
  - Power up/down (for redundant power)
  - Fan out

  - Environmental parameters (like temperature, humidity, etc.)

- How will the monitoring be done:
  - Remotely (from the provider, from a central point in the campus, etc.)
  - Locally (on site, per building, etc.)
  - Centralised
  - Distributed (per campus, building, etc.)

- What mechanisms will be used (the specific software tools do not need to be included; if they are specified, the provider should reserve the right to change them in the future):
  - SNMP
  - Syslog
  - Flow Monitoring
  - Streaming Telemetry
  - Active probes

- Where will the monitoring system/infrastructure be installed:
  - Physical platform
  - Virtual platform (VM)
  - Hybrid - Physical and virtual platform

- How will the provider manage the Network Management System (NMS) required for CNaaS:
  - From the provider
  - Through external services

- How will the customer be able to access the monitoring system (if applicable):
  - Certificate
  - Federation
  - Login/password
  - A combination of the above

- Who will install all the necessary software tools for the correct monitoring of the infrastructure:
  - The provider
  - The customer

- The set of reports that the provider will send to the customer (see Section 1.5.3).
- Needs of the monitoring system that may involve actions from the customer. For instance, the monitoring system should be:
  - Accessible to the provider (appropriate access for the provider – e.g. SNMP access, flow monitoring access, etc. – this has to be configured).
  - Able to send alerts to the providers' servers for monitoring, alerting and ticket generation (filtering at the customer may be involved).
  - Able to send emails.
  - Able to open tickets to a previously defined list of recipients.

- Able to send alerts to the alarm console.
- Accessible through any firewalls that depend on the customer.

1.4.1.2 *Monitoring of Additional Services*

The provider may offer the customer the monitoring of services that are not specific pieces of equipment or links on the network but network-related services. Regarding the monitoring of the infrastructure (see Section 3.4.1.1), the level of detail given in the service definition may vary depending on the case. For instance, it may indicate that the provider will install all the necessary software tools for the correct monitoring of the infrastructure, without listing the specific software tools.

The following lists show examples of items to be included in the service definition for the monitoring of additional services:

- List of supported additional services (other ICT services such as email, web, directory service or other servers can be out of the scope of the service):
    - DHCP
    - DNS
    - VPN
    - RADIUS
    - LDAP
    - NTP
    - VoIP
- List of parameters to be monitored for each additional service (see the list in Section 3.4.1.1 for more examples):
    - General availability.
    - Disk usage.
    - Service-specific parameters (like number of requests/s for DNS, number of authentications in Radius, number of requests in NTP, time-to-respond, etc).

The list in Section 3.4.1.1 may also be used for the monitoring of additional services.

1.4.1.3 *Configuration and Management of the Wired Network*

The provider can offer greenfield services (with new infrastructure) and brownfield services (using existing infrastructure at the customer’s premises). It is important that the provider and the customer agree on the service elements covered by this service package.

The campus architecture design typically has three layers - core, distribution and access, although the network on each campus may vary and the exact scope of the service should be defined.

The level of detail given in the service definition depends on the case. For instance, it may indicate that the provider will configure the equipment, without specifying how this configuration will be done.

The following list shows examples that can be included in the service definition for the configuration and management of the wired network:

- The network architecture, that can be designed as a part of CNaaS can:
    - Consist of three layers: core, distribution and access (for big campuses), or
    - Consist of two layers: core and access (for small campuses), or
    - Follow a two-layer Spine/Leaf topology.
    - The provider may reserve the right to further develop the architecture and network design. The customer should undertake to follow any changes these developments may require.

- Network services that can be offered as a part of CNaaS:
    - The core will be IP-based (IPv4/IPv6 access will be provided to all end users).
    - Layer 2 connectivity will be possible between any two ports in the network.
    - IP over layer 2 can be terminated in the core using separate routing policies (VRF).
    - Layer 2 connectivity over the core will be implemented using overlay techniques (VXLAN or MPLS).
    - IP can, where necessary, terminate in a firewall.

- The configuration and management:
    - For core routers, the configuration will be manually done via CLI, locally on the customer's premises.
    - For all the equipment, the setup will be automated.
    - For access switches, the setup will be automated, making the network devices acquire a temporary DHCP address through which automated scripts will configure the initial setup based on data from a centrally maintained configuration database, that can be managed by the provider or by the customer (this must be agreed in the contract between the provider and the customer).
    - For firewalls, the traffic-filtering and rate-limiting rules must be defined by the provider and the customer.
    - Standard changes in the network equipment will be automated. See Section 3.4.3.

- The bandwidth delivered to each point in the access network (depending on the ability of the customer to provide the wiring that complies with quality standards and length).

1.4.1.4 *Configuration and Management of the Wireless Network*

The provider can offer greenfield services (with new infrastructure) and/or brownfield services (using existing infrastructure at the customer's premises). It is very important that the provider and the customer agree on the service elements covered by this service package.

The level of details given in the service definition may vary depending on the case. For instance, it may indicate that the provider will configure the equipment, without specifying how this configuration will be done.

The following list shows examples of items that can be included in the service definition for the configuration and management of the wireless network:

- Architecture:
  - Centralised/Distributed/Standalone or adhoc (all the devices communicating peer-to-peer without controller or APs).
  - One/Several wireless controllers (for redundancy, due to the size of the network, etc.).
  - One/Several wireless access points.

- CNaaS can offer the customer, for instance:
  - The wireless network design will consist of a minimum of one access point.
  - The wireless network design will consist of a minimum of one controller and access point.
  - The exact number of access points and their location will be jointly reviewed by the provider and the customer.
  - The service will cover a minimum of two SSIDs: eduroam and a guest network, although more SSIDs can be defined.
  - For eduroam, differentiated access will be provided for the customer’s employees and eduroam guests.
  - The provider will assist with the setup of the customer’s profile on cat.eduroam.org, so that each user can download their own installation.

1.4.1.5 *Configuration and Management of Additional Network Services*

The provider may offer the customer the configuration and management of services that are not specific pieces of equipment or links on the network but network-related services. The level of detail given in the service definition may vary depending on the case. For instance, it may indicate that the provider will configure the additional service, without specifying how this configuration will be done.

The following list shows examples of items to be included in the service definition for the configuration and management of additional network services:

- List of supported additional network services (other ICT services such as email, web, directory service or other servers can be out of the scope of the service):
  - DHCP
  - DNS
  - VPN
  - RADIUS
  - LDAP
  - NTP
  - VoIP

- Additional network services:
  - The primary and secondary DNS servers will be managed by the provider. The resolver service will not be included.
  - The customer will be provided with a graphical user interface to interact with the service (to add DNS entries/NTP servers, etc.).

- The service configuration will be automated.
- The provider will offer their own IPv4 and IPv6 address blocks for DHCP and/or SLAAC.
- IP addresses assigned via VPN will not be on the same ranges as on the local network.

1.4.2 Service Elements

The following subsections show the items that should be agreed between the provider and the customer beforehand for each service package. These items can be changed to fit the needs of each provider, customer and service.

1.4.2.1 *Supported Network Items or Servers*

The provider, through the CNaaS service, should define, update and maintain a list of CNaaS-supported network items and servers from different vendors for each network layer and service, including minimum supported software and hardware versions. This list should include the support of standard protocols, agreed by the provider and the customer during the design stage. The list of supported network items or servers should include, for instance:

- Switches
- Routers
- Firewalls
- Wireless controllers
- Servers
- Network Attached Storage systems
- Radio links

It is recommended that the provider offers the service using automation tools that facilitate the replication of the configuration in the network items and servers, and has a configuration management system (CMS) with the databases and tools to manage all configuration data. Thus, for instance, every time a new device is included in the CNaaS service, it can be registered in the system through the mechanism provided by the provider, which should automatically generate the monitoring configuration.

The network equipment or servers of brownfield services also needs to be included in the list of supported network items or servers.

1.4.2.2 *Equipment Procurement*

The provider and customer can agree four possible models for the equipment procurement, depending on who is making the specification and who is running the procurement and owns the equipment:

- The provider makes the equipment specification and runs the procurement.
- The customer makes the equipment specification and runs the procurement.
- The provider makes the equipment specification and the customer runs the procurement.
- The customer makes the equipment specification and the provider runs the procurement.

As an equipment specification made only by the customer might lead to incompatibilities between the procured equipment and the provider’s expertise, the provider and the customer may also need to jointly work on the equipment specification.

1.4.2.3 *Equipment Ownership*

There are two possibilities, once the procurement is done:

- The provider owns the equipment
- The customer owns the equipment

The ownership of the equipment must be agreed beforehand.

1.4.2.4 *Physical Installation of the Equipment*

There are two main options related to the physical installation of the equipment:

- The provider will be responsible for the physical execution of the work, including but not limited to assembly and connection of equipment, restart of power on equipment etc.
- The customer will be responsible for the physical execution of the work, including but not limited to assembly and connection of equipment, restart of power on equipment etc.

A third scenario with shared responsibility is also possible. For instance, the initial installation is done by the provider, but later smaller changes, cable patching and so on is done by the customer or a third party under the customer's responsibility. For any of the options, it is important to clearly define the responsibilities of both sides to avoid any misunderstanding.

1.4.2.5 *Level of Redundancy*

The level of redundancy must be specified for each supported package, layer and service. For instance, there may be some redundant elements in a layer that are not redundant in another layer. Some examples are:

- Redundant/non-redundant core layer (redundancy is highly recommended for the core network).
- Redundant/non-redundant distribution.
- Redundant/non-redundant access.
- All core equipment will have redundant power supplies, fans, supervisors, etc.
- All the core links will be redundant.
- The redundant architecture will include network elements and links at all levels except access ports.
- The architecture is partially redundant, with redundancy in some network elements or links (that need to be specified).
- The wireless network service will have redundant controllers.

1.4.2.6 *Software Tools*

CNaaS will use a set of tools that will be defined by the provider and does not need to be included in the service definition, although it is up to the provider to include them if desired.

Different tools may be used for:

- Customer Relationship Management (CRM)
- Monitoring
- Ticketing
- Inventory
- Configuration management and backup
- Billing

The integration between the different tools can be defined.

Due to the nature of the CNaaS service, it may be necessary to have a database tool for the location of buildings, room numbers, locally specific information, rack access keys, etc.

1.4.3 Change Management

The exact scope of the required changes related to any part of the CNaaS service should be defined in advance. It is suggested to follow the ITIL recommendations and processes for change management [ITIL-CM]. What will be considered a standard change (pre-authorised, with an accepted and established procedure, possibly automated), a normal change (requires a Request For Change (RFC) and/or the CAB approval) or an emergency change (must be introduced as soon as possible, requires ECAB approval) should be identified. Once identified, different changes can be included in the service (for instance, those changes that can be automated), while others can be excluded (like manual or complex changes). Some examples of the type of changes that could be included or excluded are given below.

The service can include the following standard changes:

- Software upgrades.
- Changing common global configuration parameters like NTP server, console password, etc.
- Adding new VLANs with attributes.
- Adding or changing routed IP prefixes.
- Provisioning security measures.
- The VLAN for any port in the wired network.
- The SSID for the wireless network.
- The access-lists rules for core equipment.
- Security rules in the firewalls.
- DNS modifications.
- Other type of change agreed between the provider and the customer.

The service does not include the following changes:

- The core architecture routing design.
- The wireless setup on the individual client.

The list of changes should be regularly reviewed, re-negotiated and updated as appropriate.

1.4.4 Incident Management

An incident is defined as an unplanned interruption of the service, or the failure of a service component that has not yet impacted the service. A problem is a cause of one or more incidents. The aim of incident management [ITIL-IM] is to restore the service to normal service operation as quickly as possible through a workaround or a permanent solution to the problem. A definition of what normal service operation means is desirable (for instance, whether any packet loss or jitter in the service is acceptable).

1.4.4.1 *Types of Incident*

The incidents are usually classified in categories according to their impact and urgency, and given priority levels. The provider must offer a way to classify incidents to the customer. Common ways to classify incidents are:

- Non-critical/Critical
- Low/Medium/High
- Very Low/Low/Medium/High/Critical

For instance, an incident can be considered critical if the service is not reachable at all or degraded by more than <n%> packet loss, has more than a specified jitter or latency between two fixed points or affects certain critical customers.

A special type of high priority incident is a major incident. Major incidents have a direct impact on the business (they typically affect a lot of customers simultaneously / affect VIP customers / affect the customer's reputation) and should trigger a specific process to handle them.

1.4.5 Support Service

The provider and the customer should agree the level of the support service that will be provided, including clear steps to take for each type of incident. Such an agreement could include the following elements:

- Number of hours per day
- Service support over weekends and holidays
- Calendar (holidays should be taken into account and they may be local to a city or a region)
- Response time
- Resolution time

Some common options are:

- 24x7: The support service will be offered 24 hours a day, 7 days a week, with a response time of 1 hour and a resolution time of 4 hours from the registration of the incident.
- 8x5 next business day (NBD): The support service will be offered 8 hours a day (from XX:XX to YY:YY), 5 business days a week, except holidays, with a response time of 1 hour and a resolution time of 4 working hours from the registration of the incident.

The provider and the customer should agree the different levels of the support service that will be provided. For instance:

- The helpdesk will be run by the customer and will provide a single point of contact for all trouble ticket reports.
- The provider will offer second- and third-line operations and the support service must be operated in collaboration with the IT staff/helpdesk at the institution, which will provide the first-line support.
- During the operation stage, the NOC, in coordination with the customer helpdesk, will follow the daily operations of the networks (events, incidents, problems) on a 24x7 basis.

1.5 Service Policy

It is important to define the Key Performance Indicators (KPI) that will be used to measure the quality of the service and the expected Service Level Targets (SLT). The following subsections show some examples of parameters and paragraphs that can be included in the service definition regarding service level management [ITIL-SLM], provider/customer responsibilities and communication flows.

1.5.1 Service Level Management and Service Availability

To measure the quality and the performance of the service, relevant objective parameters and expected scheduled downtimes need to be agreed beforehand.

1.5.1.1 *Key Performance Indicators (KPI)*

Key Performance Indicators (KPI) need to be defined per time period for service level management. Some examples are:

- Number of incidents
- Number of problems
- Number of implemented standard changes (not approved by the CAB)
- Number of implemented normal changes
- Number of implemented emergency changes
- % of changes that caused incidents
- Average change closure duration (between Request For Change (RFC) is raised and closed)
- Average time to respond to an RFC
- Average time to solve critical incidents

- Average time to solve non-critical incidents
- Average time to close request tickets (information, documentation)
- Average time to solve problems

The exact list of KPIs and the time period must be agreed between the provider and the customer. It can be reviewed and re-negotiated as needed and the contract should be updated accordingly.

1.5.1.2 *Service Level Targets (SLT)*

For each service package, availability is defined as the total number of minutes in a calendar month during which the service is available, divided by the total number of minutes in a calendar month and represented as a percentage.

The Service Level Target (SLT) for CNaaS availability for a certain period should be agreed (for instance, <n%> monthly availability) [ITIL-SLM], ignoring planned maintenance windows.

If there are any constraints, they should also be stated in the contract. For instance, if the helpdesk is responsible for opening incidents and escalating them to the second level when needed, the expected SLA times for incidents will begin once the incident is escalated to the second level (for instance, via the ticketing system).

The following are examples of SLTs that can be defined:

- The time to respond to a critical incident ticket target (for instance, 30 minutes).
- The time to respond to a non-critical incident target (for instance, 24 hours).
- The time to respond to a request target (for instance, 24 working hours).
- The time to fix a critical incident target (for instance, 4 hours).
- The time to fix a non-critical incident target (for instance, 48 hours).
- The time to make a change; target times are (RFC required):
  - For standard changes (for instance, 48 hours).
  - For normal changes (for instance, 2 weeks, after the CAB has accepted the change).
  - For emergency changes (for instance, 2 hours, after the ECAB has accepted the change).

The exact list of SLTs and the time period must be agreed between the provider and the customer. It can be reviewed and re-negotiated as needed and the contract should be updated accordingly.

1.5.1.3 *Scheduled Downtimes*

The provider should inform the customer how scheduled downtimes will be handled. For instance:

- Scheduled downtimes or planned maintenance windows will be accepted by the CAB, except for emergency changes, that will be accepted by the ECAB.
- Once agreed, downtimes will be announced by the provider via email at least <n> days before they happen, except for emergency changes, which will be announced as soon as possible. They will include the reasons for the scheduled maintenance and the expected downtime.

- Upgrades and replacements in the core and distribution layers can be done during working hours (for instance, if all architecture components are redundant). The access layer maintenance tasks will need to be agreed with the customer (as access ports are not usually redundant).

A specific maintenance window can be agreed for some tasks. Pre-agreed weekly or monthly windows can be defined during the design stage, so that maintenance tasks are always performed during this time slot. Then, the provider will only have to inform the customer of the task, date and duration of the task.

1.5.2 Responsibilities

The responsibility demarcation point between the provider and the customer should be defined. For instance, for the wired network it can be the port on the managed equipment towards the infrastructure managed by the customer.

The service definition should clearly reflect the provider and the customer responsibilities.

1.5.2.1 *Service Provider Responsibility*

The provider can be responsible for, for instance:

- At least one on-site visit to get to know the network before starting to offer CNaaS services.
- Managing the equipment and services specified in the service description within the boundaries of the KPIs defined for the service.
- The correct patching update of the network items managed by the provider, in order to avoid security leaks. If an upgrade on a CNaaS-covered device triggers an update on a customer-managed device, the provider and the customer should collaborate and coordinate the actions to prevent the service from being affected.
- Providing and maintaining the issue tracking system (trouble-ticketing system) for the second and third level support that the provider is responsible for.
- Providing procedures for RFCs, issue and problem reporting.
- Responding to justified RFCs according to the defined KPIs on the managed equipment from the service customer.
- Responding to service customers’ problem and incident reports according to the defined KPIs.
- Providing and maintaining the tools required for providing this service and managing automation.
- Providing second and third line support for the issues reported by service customers.
- Maintaining the technical logs with information about the network items, services and servers and ensuring appropriate information security for these logs.
- Maintaining a central Configuration Management Database (CMDB) for all network equipment and services.

The service provider will not be responsible for, for instance:

- The performance or incidents on external links or pieces of equipment not covered by the CNaaS agreement (like cloud services, multi-tier structures, testbeds, etc.).
- The information security of the end-user devices.
- Small changes to the customers physical infrastructure (e.g. patch cables, power supplies and cabling).
- Establishing appropriate environmental conditions for the equipment stored on customer premises (temperature humidity).
- Providing fire-protecting infrastructure and policies at the customer site.
- The configuration setup and management of the local customer devices not included in the service.

1.5.2.2 *Service Customer Responsibility*

The customer can be responsible for, for instance:

- The passive network infrastructure within the campus (cabling, patch-panels, racks and the like).
- The operation and up-to-date configuration of any ICT equipment (e.g. switches, routers, computers, laptops, servers, IP telephones, access points, etc.) at the campus that is not explicitly listed as being managed by the service provider.
- The information security of the ICT equipment at the campus listed in the previous bullet (e.g. patching software, applying antimalware software and similar).
- Controlling physical access to the equipment managed by the provider. Access can be allowed only to authorised persons employed by the provider, customer or equipment vendor. The list of authorised persons will be agreed between the customer and the provider. The procedure for the physical access should also be agreed, including:
  - Authorisation procedure.
  - Changing the list of authorised persons.
  - Access logging.
  - Information sharing about physical access - who should receive / acknowledge / approve the physical access to the devices.
- Allowing service provider personnel physical access to the managed equipment.
- Maintaining the environmental conditions (e.g. temperature, humidity, power consumption) of all the ICT equipment at the customer’s facilities managed by the service provider within the boundaries defined by equipment manufacturer.
- Following fire safety guidelines (e.g. having enough gas for fire suppression in the data centre or assistance for fire extinction).
- Planning the location of Wi-Fi access-points appropriately, according to building and fire regulations guidelines.
- Executing simple operations on managed equipment (e.g. power cycle, changing the patch cable, and similar) upon the request or with the permission of the service provider.

- Actively participating in debugging and problem-solving activities on managed ICT equipment by timely providing relevant information to the service provider, especially upon the request from the service provider and executing previously agreed simple operations.
- Following the RFC and issue reporting procedures and using the problem and issue reporting tools specified by the service provider.
- Providing the first line of support to the users of the campus network. The provider will not react to calls from the campus network's end users. The customer should designate authorised persons to communicating with the provider.
- Any potentially malicious end user activities.
- Informing their users of all relevant procedures and policies, of how the network and the resources should be used, including - if appropriate - relevant elements of the contract between the provider and the customer.
- Supporting the CNaaS service on-site and providing a point of contact for all trouble ticket reports (if the helpdesk is run by the customer).

The customer will not be responsible for, for instance:

- The configuration and management of the equipment under the CNaaS agreement.

1.5.3 Communication Flows

The provider and the customer should define the communication channels for the defined roles and the communication flows in the contract. The following subsections provide some examples.

1.5.3.1 *Communication Flows for Service Level Management*

As part of the Service Level Management, the provider and the customer should agree the communication flows required for reviewing the quality of the service.

The following list gives some examples:

- Regular/On-demand meetings:
  - The Service Manager from the provider's CNaaS team and the Service Coordinator from the customer team should meet regularly (face-to-face or remotely via VC) to follow-up on service requirements and possible improvements.
  - The Service Coordinator or the Service Managers can set a maximum of <n> adhoc meetings per month if needed.

- Regular/On-demand reports:
  - Based on the monitoring and the logs, the Service Manager will periodically (or at customer request, if preferred) provide customer with the following reports, which can be automatically generated if possible:
    - Availability statistics.
    - SLT and KPI review results, including SLA violations, if any.
    - Service improvement plan.
    - Incident report.

  - The customer can ask for special incident reports in relevant cases, with a maximum of <n> incident reports per month.

- Complaints or special cases:
  - Complaints will be sent to the Service Manager and discussed during regular meetings, unless an urgent incident requires a special meeting.
  - In case of relevant critical incidents, either side can require special meetings with a representative of the other side.

1.5.3.2 *Communication Flows for Incident Management*

The provider and the customer should agree the alarm and ticket recipients and escalation procedures, which will depend on the defined resolution times (see Section 3.4.5).

Alarm Recipients

Several options can be considered:

- Alarms triggered on the monitoring system will be sent to the alarm console at the helpdesk and open a ticket in the helpdesk system.
- Alarms triggered on the monitoring system will be sent to the alarm console at the provider's NOC.
- Alarms triggered on the monitoring system will be sent to the alarm console at the provider's NOC and the helpdesk, and open a ticket in the helpdesk system.

The monitoring system can automatically send notifications to the customer helpdesk and, while the monitoring system cannot monitor itself, the central monitoring system at the provider can issue notifications if the monitoring system itself has a failure.

The provider and the customer may agree on different recipients depending on the nature of the alarms (for instance, when major incidents are detected). Alarms can also trigger automatic calls or send text messages.

Ticket Recipients

There are several options:

- The helpdesk receives the alarms.
- The provider's NOC receives the alarms.
- Both the helpdesk and the NOC receive the alarms.

Escalation Procedures

The escalation procedures between the provider and the customer in case of an incident should be defined and agreed by both parties. For instance:

- The Service Coordinator at the customer may escalate the incident to the Service Manager or the Product Manager at the provider when an incident is not solved in the agreed resolution time or when a major incident occurs. Some common options are to escalate to the:
  - Service Manager if the incident is not solved within the agreed resolution time.

    - Service Manager if an incident reaches the Service Level Target (SLT).
    - Product Manager if the incident is not solved within the agreed resolution time plus <n> hours.
    - Product Manager if an incident reaches the SLT twice.
    - Product Manager if a major incident occurs.
    - Provider Chief Technical Officer (CTO, Management) if an incident reaches the SLT three times.

- If an issue is escalated, the incident must be sent to the provider's NOC (for instance, via the Trouble Ticketing System).

1.6 Duration, Changes and Termination

The contract should include information about the service's duration, the scope for the provider and customer to make changes to the service during the contract period and causes for termination. Both parties could request advice from their legal specialists.

Some examples are:

- Duration of the service:
    - The service will begin when the agreement is signed and will remain in effect for an initial term of <n> months / years.
    - This service only applies to the pilot period in the project CNaaS (if it is a project) for the duration of <n> months / years.

- Possibilities to change the service:
    - The agreement may not be modified, amended, changed or discharged, in whole or in part, except by an agreement in writing signed by the provider and the customer.

- Renewals:
    - The agreement will automatically renew for successive <n> years unless the provider or the customer provide at least <n> days prior written notice to the other party of their desire not to renew the agreement.

- Causes for termination:
    - The provider or the customer may terminate the agreement immediately should the other party admit in writing its inability to pay its debts as they become due.

- Notice period for termination:
    - In the event either party desires to terminate this agreement or any of the associated services, the party shall provide at least <n> days written notice of the termination date to the other party, unless the receiving party agrees, in writing, to a shorter notice period.

1.7 Prices and Billing

Several charging model options are possible and can be added or combined according to the offered services. Some examples are:

- Fixed fee (one-off, monthly, annual, etc.).
- Variable charging (depending on the number of tickets, requests, number of users, number of students, connected buildings, etc.).
- Free of cost (included in the basic connectivity quota, paid by the government, etc.).
- Part of the connection fee to the NREN.
- Specific quota for each service package.
- Specific quota for each managed device, additional service, building, users, etc.

The provider can generate a price list of the different options offered to the customers.

The billing periods, if applicable, also must be defined. For instance:

- Monthly
- Quarterly
- Yearly

1.8 GDPR Privacy Notice

Depending on where sensitive data is stored and whether the provider has access to it, different policy notices may be used. In the process of the GDPR assessment, the usage of the <service_name> data inventory template [Template] and GDPR templates [GDPRtemplate] from the GÉANT wiki may be helpful in determining what data is processed that the GDPR applies to. Both the provider and the customer should obtain the advice of their GDPR specialists.

In some cases, a separate contract that regulates the relationship between the controller (the organisation that determines the purposes of the processing of personal data) and the processor (the organisation that processes the data) might be needed, especially if the provider uses subcontractors (e.g. a company that maintains servers or storage where the customer's monitoring data is stored) which could obtain access to the customer's personal data. The following paragraphs are an example of what should be defined for each service package.

1.8.1 What Data is Processed?

The provider and the customer should agree who is keeping CNaaS-related logs of events in the network items, servers, services and monitoring system(s), and who is able to access the logs for troubleshooting. These logs should contain at least the following data:

- The network item, server or service involved.
- The date and time of the event.

- The IP address of the user.

The data controller of this data should also be specified.

1.8.2 Purposes of the Processing

Logs are kept to investigate and solve network problems and incidents, open tickets and collect aggregate statistics about the services.

The CNaaS provider has no means to correlate technical log data with personal data. The provider will not provide technical log data to anyone, unless ordered to do so by law, for example as part of a criminal investigation.

The legal basis for processing personal data is the customer’s consent.

1.8.3 Consent

The customer consents to have the data listed in Section 1.8.1 logged by the provider.

1.8.4 Data Storage

All the data is stored within the EEA (European Economic Area).

1.8.5 Retention Period

The provider and the customer should agree on the retention period of technical logs of transactions. For instance, a period of 6 months or 1 year from the date of the event.

1.8.6 Security of Data

Access to the technical logs data is restricted and can only be accessed by CNaaS staff. To prevent unauthorised access or disclosure, the provider has put in place technical and organisational procedures to secure the data collected.

1.8.7 Customer Rights

The customer may request a copy of the technical log data the provider is storing of the events as described in Sections 1.8.4 and 1.8.5.

1.8.8 Changes to this Notice

This privacy statement may be changed at the provider’s discretion at any time. If the provider makes changes to this notice, the last modified date is updated, and the customer notified.

References

[AXELOS] https://www.axelos.com/

[D6.2] Deliverable D6.2 *Automation and Orchestration of Services in the GÉANT Community* https://www.geant.org/Projects/GEANT_Project_GN4-3/GN43_deliverables/D6-2_Automation-and-Orchestration-of-Services-in-the-GEANT-Community.pdf

[GDPRtemplate] https://wiki.geant.org/display/gn43wp6/GDPR+Templates (Note that eduGAIN credentials are required to access this page)

[ITILv3] ITIL® Service Lifecycle Publication Suite, 2011 Edition, ISBN: 9780113313235

[ITILv4] https://wiki.en.it-processmaps.com/index.php/ITIL_4

[ITIL-CM] ITIL® Service Transition, 2011 Edition, ISBN: 9780113313068

[ITIL-IM] ITIL® Service Operation, 2011 Edition, ISBN: 9780113313075

[ITIL-SLM] ITIL® Service Design, 2011 Edition, ISBN: 9780113313051

[Template] https://wiki.geant.org/display/gn43wp6/%3Cservice_name%3E+data+inventory+Template (Note that eduGAIN credentials are required to access this page)

[WIFIMON] https://www.geant.org/wifimon

Glossary

CAB	Change Advisory Board
CI/CD	Continuous Integration/Continuous Delivery
CLI	Command-Line Interface
CMDB	Configuration Management Database
CNaaS	Campus Network Management as a Service
CRM	Customer Relationship Management
CTO	Chief Technical Officer
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ECAB	Emergency Change Advisory Board
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronics Engineers
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITIL	Information Technology Infrastructure Library
KPI	Key Performance Indicator
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MPLS	Multiprotocol Label Switching
NMaaS	Network Management as a Service
NOC	Network Operations Centre
NTP	Network Time Protocol
NREN	National Research and Education Network
OAV	Orchestration, Automation and Virtualisation
perfSONAR	Performance focused Service Oriented Network monitoring ARchitecture
PMP	Performance Measurement Platform
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Change
SIG	Special Interest Group
SIG-NOC	Special Interest Group - Network Operation Centres
SLA	Service Level Agreement
SLT	Service Level Target
SNaaS	School Network Management as a Service
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
VC	Video Conference
VLAN	Virtual Local Area Network
VM	Virtual Machine

VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
VRF	Virtual routing and forwarding
VxLAN	Virtual Extensible LAN
WIFI	Family of wireless networking technologies defined in IEEE 802.11x
WiFiMon	Wireless Crowdsourced Performance Monitoring and Verification
WP	Work Package
ZTP	Zero Touch Provisioning