GÉANT
Networks • Services • People

CNaaS Service Definition

Maria Isabel Gandia, CSUC/RedIRIS
GN4-3 WP6 T3 / CNaaS

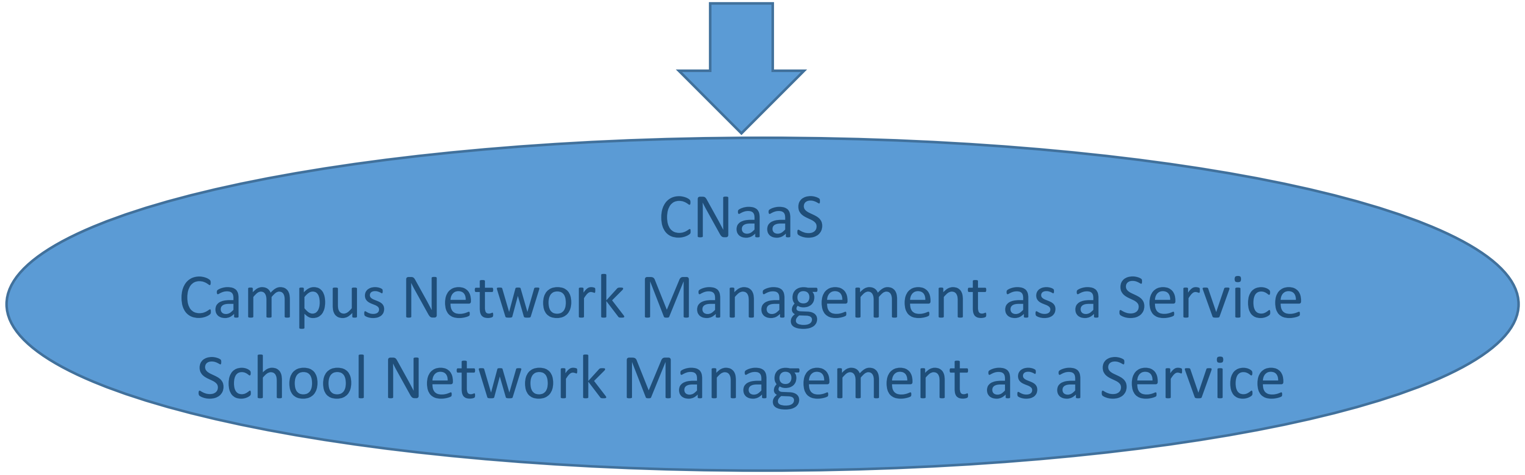
Workshop on Network Management and Monitoring

Copenhagen, 21 October 2019

www.geant.org

Why CNaaS?

- NRENs have good reputation for the management of their own infrastructure.
- Lack of qualified network technicians in the end-institutions connected to the NRENs.
- Difficulties in recruiting network technicians.
- Government initiative or project.



CNaaS

Campus Network Management as a Service

School Network Management as a Service

The scope of the work must be agreed!

- The provider and the customer can sign a contract or a Service Level Agreement (SLA) or the provider can have some standard fixed offers. The provider and the customer must define and agree on:
  - What is included in the service in the basic package.
  - What is added as an extended or supported package.
  - The demarcation points between the provider and the customer.
  - How to measure the quality and availability of the service.
  - Customer and provider responsibilities.
  - …

The CNaaS Service Definition Document

- Many NRENs/providers are already offering CNaaS services:

Some common ideas…	…but doing things in different ways
Good reputation for network management	Approach
Need to offer CNaaS Services	Offered services
Need to have a clear Service Definition	Configuration mechanisms
Hard to begin from scratch	Tools
Willing to share experiences and learn	Scope

- Making a single Service Definition (SD) Document “that fits them all” was complicated.
- The purpose is to provide ideas and create an SD Document as a template for each provider, easy to adapt and replicate.
- When writing its own SD Document, the provider can modify the text and adapt the examples.
- It can also be used as a reference when writing the contract or Service Level Agreement.

The structure of the CNaaS SD Document

1. Introduction
2. Terminology
3. Contacts/Roles
4. Service Delivery Model
5. Service Policy
6. Duration, Changes and Termination
7. Prices and Billing
8. GDPR Privacy Note
9. References

https://wiki.geant.org/display/gn43wp6/CNaaS+Service+Definition+Template

2. Terminology

- Some short definitions for:
  - Provider
  - Customer
  - Supported Service
  - Supported Network Items and Servers
  - Additional Network Services
  - Network Management and Monitoring System

3. Contacts/Roles

- Suggested roles for the provider:
    - Product Manager
    - Service Manager
    - Technical Advisor
    - NOC team

- And for the customer
    - Service Responsible
    - Helpdesk team

During the Service Design stage, they should meet and define:

- Scope
- Involved packages
- Architecture
- Expected timeline
- SLAs
- …

- The members of the Change Advisory Board (CAB) and Emergency Change Advisory Board (ECAB) can also be defined.

4.Service Delivery Model (index)

4.1 Supported Service Packages

- 4.1.1 Monitoring of the Infrastructure
- 4.1.2 Monitoring of Additional Services
- 4.1.3 Configuration and Management of the Wired Network
- 4.1.4 Configuration and Management of the Wireless Network
- 4.1.5 Configuration and Management of Additional Network Services

4.2. Service Elements

- 4.2.1. Supported Network Items or Servers
- 4.2.2. Equipment Provisioning
- 4.2.3. Physical Installation of Equipment
- 4.2.4. Level of Redundancy
- 4.2.5 Software Tools

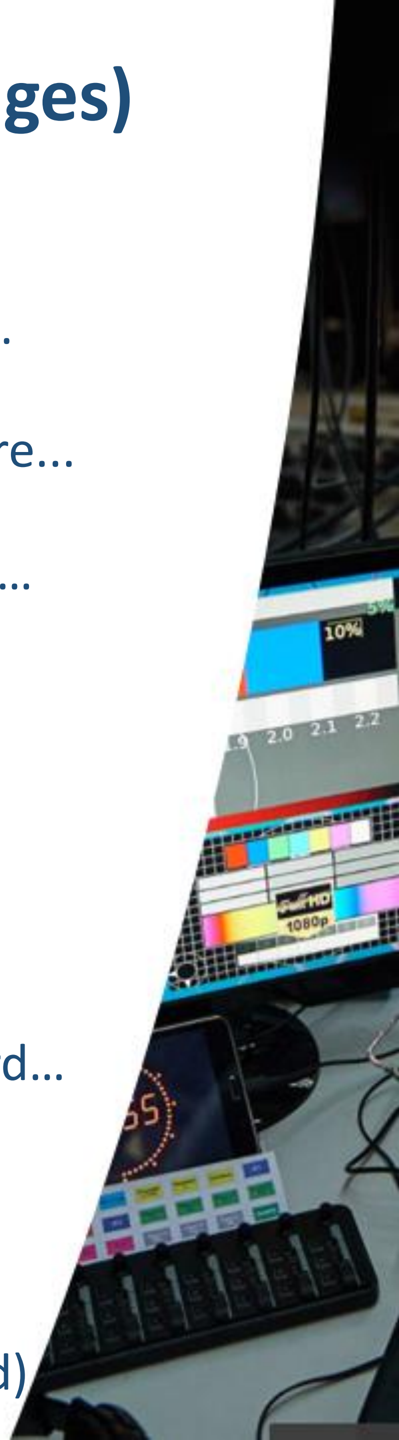
4.3. Change Management

4.4. Incident Management

- 4.4.1. Types of incidents
- 4.4.2. Support Service

4.1.1 Monitoring of the Infrastructure (Supported Service Packages)

•What will be monitored?	Routers, Switches, FW, Access-points…
•What will the monitoring system do?	Trigger alarms, generate graphs, reports…
•What parameters will be monitored?	CPU, memory, traffic, latency, temperature...
•How will the monitoring be done?	Remotely, locally, centralized, distributed…
•What mechanisms will be used?	SNMP, Syslog, FlowMon, Telemetry...
•Where will it be installed?	Physical platform, VM, several VM…
•How will the monitoring be monitored?	From the provider, external services…
•How will the customer access it?	Certificate, federation, login and password…
•Who will install the software tools?	The provider, the customer…
•Needs of the monitoring system that may involve actions from the customer?	Accessible for the provider, able to send alerts, e-mails… (filtering may be involved)



4.1.2. Monitoring of Additional Services (Supported Service Packages)

- List of supported additional services?

DHCP, DNS, VPN, RADIUS, LDAP, NTP, VoIP...

- What parameters will be monitored for **each** additional service?

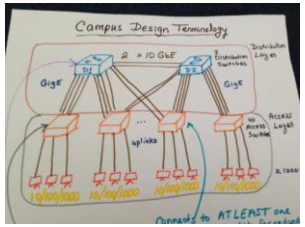
General availability, Disk usage, number of requests/s for DNS, number of authentications in Radius, number of requests in NTP…

The bullet list from the previous section may be used for the monitoring of additional services.

4.1.3. & 4.1.4. Config and Management of the Wired/Wireless Network

- What is the architecture?

Core/Distribution/Access, Leaf/Spine…



- What will be offered to the customer?

IPv4/IPv6 access to end users / <n> access-points and 1 controller, 2 SSID…

- How will the configuration and management be done?

The setup will be automated / for core routers, the setup will be done locally…

- What bandwidth will be delivered to each point in the access network (wired)?

100 Mbps/1 Gbps, depending on the ability of the customer to provide the wiring that complies with quality standards and length…

4.1.5. Configuration and Management of Additional Network Services

• List of supported additional services?	DHCP, DNS, VPN, RADIUS, LDAP, NTP, VoIP...
• What will the service offer for each additional network service?	Primary and secondary DNS servers (resolver not included)/ GUI to interact with the service, IPv4 and IPv6 address blocks for DHCP…

The bullet list from the previous section may be used for the configuration and monitoring of additional services.

4.2.1. Supported Network Items or Servers (Service Elements for each SP)

• List of supported network items and servers from different vendors?	Switches, Routers, Firewalls, Wireless controllers, Servers, NAS systems, Radio links…
• Minimum supported software and hardware versions?	AX2300, OS v2.0 BZ5400, UOS v3.1.3…

⚠ The list should be defined, updated and maintained by the provider

Having this list facilitates the use of automation tools

4.2.2. Equipment Provisioning (Service Elements for each SP)

- Possibilities:

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.

A joint work for the specification is also possible.

⚠ *An equipment specification made only by the customer might lead into incompatibilities between the procured equipment and the provider expertise!

4.2.3. Physical Installation of Equipment

- Physical Installation: assembly and connection of equipment, restart of power on equipment and the like.
- Possibilities:

The provider will be responsible for the physical installation

The customer will be responsible for the physical installation.

- A third scenario with shared responsibility is also possible (for instance, the initial installation is done by the provider, but later small changes, are done by the customer).

4.2.4. Level of redundancy

- Level of redundancy?

Redundant/non-redundant core /distribution /access layer, redundant power supplies, fans, supervisors, core links, redundancy at all levels except access ports, no redundancy….

⚠ The level of redundancy must be specified for each supported package, layer and service.

Be redundant,
be redundant

4.2.5. Software Tools

- The provider will use a set of tools (for CRM, Monitoring, Ticketing, Inventory, Configuration management and Backup, Billing…) that do not need to be included in the SD.

- The integration between tools may also be defined.

It's up to the provider to include as many technical details as desired, although if many details are given, they are more likely to change in the future. 😉

4.3. Change Management

- The exact scope of the required changes should be defined in advance.

Standard Change

- Pre-authorised
- With an accepted established procedure
- Possibly automated

Normal Change

- Requires a Request For Change (RFC)
- and/or the CAB approval

Emergency Change

- Must be introduced as soon as possible
- Requires ECAB approval

- The list of included changes must be defined and can be adjusted depending on the needs from any of the sides.

4.4. Incident Management (4.4.1 Types of incidents & 4.4.2 Support Service)

- Classification of incidents?

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

- Level of the support service (number of hours per day, calendar, response & resolution time)?

24x7, 8x5 NBD, 30 min response & 4 h resolution for critical incidents, 1 h response and 24h resolution for Non-critical incidents…

- How will the service be offered?

Helpdesk run by the customer and 2nd & 3rd line by the provider / the NOC, in coordination with the customer Helpdesk will follow the daily operations of the networks on a 24x7 basis…

5. Service Policy (index)

- 5.1. Service Level Management and Service Availability
  - 5.1.1. Key Performance Indicators (KPI)
  - 5.1.2. Service Level Targets (SLT)
  - 5.1.3. Scheduled downtimes
- 5.2. Responsibilities
  - 5.2.1. Service Provider Responsibility
  - 5.2.2. Service Customer Responsibility
- 5.3. Communication Flows
  - 5.3.1. Communication Flows for Service Level Management
  - 5.3.2. Communication Flows for Incident Management
  - 5.3.2.1. Alarm Recipients
  - 5.3.2.2. Ticket Recipients
  - 5.3.2.3. Escalation Procedures

5.1.1. Key Performance Indicators (KPI) & 5.1.2. Service Level Targets (SLT)

- Key Performance Indicators (KPI)?

Number of incidents, number of problems, number of implemented normal changes, average time to solve critical incidents, average time to solve non-critical incidents…

- Service Level Targets (SLT)?

Monthly availability, time to respond to a critical incident ticket target, time to respond to a non-critical incident target, time to respond to a request, time to fix a critical incident target, time to do a change target…

5.1.3. Scheduled Downtimes (Service Availability)

- How will scheduled downtimes be handled?

Maintenance windows will be accepted by the CAB, emergency changes will be accepted by the ECAB / Downtimes will be announced by the provider via email at least <n> days before they happen, emergency changes, will be announced as soon as possible / Upgrades and replacements in the core and distribution layers can be done during working hours / The access layer maintenance tasks will need to be agreed with the customer.

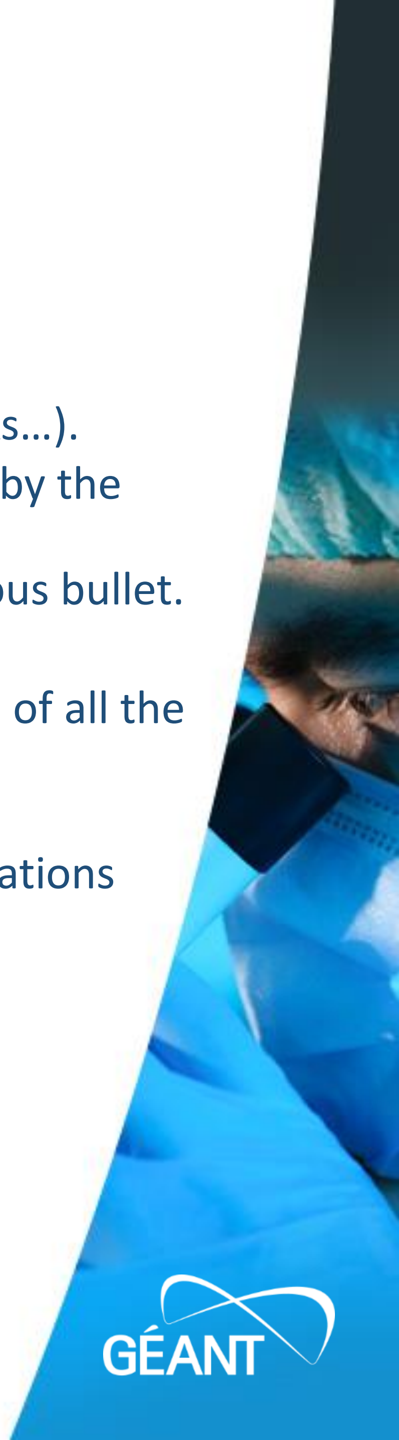
⚠ A pre-agreed maintenance window can be defined.

5.2.1. Service Provider Responsibility

- The provider will be responsible, for instance:
  - For at least one on-site visit before deploying CNaaS.
  - To manage the equipment and services within the boundaries of KPI defined for the service.
  - For the correct patching update of the network items managed by the provider.
  - To provide and maintain the issue tracking system for the 2nd and 3rd level support.
  - To provide procedures for Requests For Changes, issues and problem reports.
  - To respond within the KPI boundaries to the justified Requests For Changes on the managed equipment.
  - To respond within the KPI boundaries to the reports about the problems and incidents.
  - To provide and maintain all the tools required for providing this service and manage automation.
  - …
- The service provider won't be responsible, for instance:
  - For the performance or incidents on external links or pieces of equipment not covered by the agreement (like cloud services, multi-tier structures, testbeds...)
  - …

5.2.2. Service Customer Responsibility

- The customer will be responsible, for instance:
  - For the whole passive network infrastructure within the campus (cabling, patch-panels, racks…).
  - For the operation and up-to-date configuration of all the equipment not explicitly managed by the provider.
  - For the information security of all the ICT equipment in the campus mentioned in the previous bullet.
  - To restrict and control the physical access to the equipment managed by the provider.
  - To maintain the environmental conditions (e.g. temperature, humidity, power consumption) of all the equipment.
  - To follow fire safety guidelines (like having enough gas for fire suppression).
  - To plan the location of Wi-fi access-points appropriately, according to building and fire regulations guidelines.
  - To provide the 1st line of support to the users of the campus network.
  - …
- The customer won't be responsible, for instance:
  - For the configuration and Management of the equipment under the CNaaS agreement
  - …



5.3.1. Communication Flows for Service Level Management

- Regular meetings?

The Service Manager will regularly meet with the Service Responsible to follow-up with the needs of the service and possibilities of improvement…

- Regular/on-demand reports?

The Service Manager will periodically provide reports: Availability statistics, SLT and KPI review results, 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 the regular meeting/In case of relevant critical incidents or complaints, any side can require extraordinary meetings with the representative of the other side…

5.3.2. Communication Flows for Incident Management

- Alarm recipients & Ticket recipients?

Helpdesk/NOC/Both

- Escalation procedures?

Service Manager if the incident is not solved in the agreed resolution time (+<n>), if the Service Level Target (SLT) is reached…/ Product Manager when <n> times the SLT is reached, if there is a major incident…/ CTO, Management when <n+1> times the SLT is reached…/ In case there is an escalation on some issue, it must be sent to the provider NOC via the Trouble Ticketing System…

6. Duration, Changes and Termination

- Duration of the service?

The service will remain in effect for an initial term of <n> years / This service only applies to the pilot period in the project…

- Possibilities to change the service?

It may not be changed or discharged, in whole or in part, except by an agreement in writing signed by the provider and the customer…

- Renewals?

It will automatically renew for successive <n> years terms unless the provider or the customer provide written notice of its desire not to renew the agreement at least <n> days prior written notice to the other party…

- 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…

7. Prices and Billing

- Charging model?

Fixed fee (one-shot, monthly, …) / variable charging (depending on the # of tickets, requests, users, students, buildings...) / free of cost / part of the connection fee…

- Billing periods?

Monthly, quarterly, yearly...

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

8. GDPR Privacy Note

- 8.1.1. What Data is Processed?
- 8.1.2. Purposes of the Processing
- 8.1.3. Consent
- 8.1.4. Data Storage
- 8.1.5. Retention Period
- 8.1.6. Security of Data
- 8.1.7. Customer Rights
- 8.1.8. Changes to this Notice

8. GDPR Privacy Note

What Data is Processed?	IP addresses, service involved…
Purposes of the Processing?	Solve incidents, collect statistics…
Consent?	The customer consents to have the data logged by the provider…
Data Storage?	All the data is stored within the EEA…
Retention Period?	6 months, 1 year…
Security of Data?	Data can only be accessed by CNaaS staff…
Customer Rights?	The customer may request a copy of the logs…
Changes to this Notice?	Privacy statement may be changed by the provider…

9. References

- AMRES
- ARNES: https://geant.app.box.com/s/68pzsqbkbcx9683j8qybgoi5zlu7jhtz
- CARNET: https://www.e-skole.hr/en/results/adequate-ict-infrastructure-in-pilot-schools/
- FUNET has started the Kampus Service project, with 7 customers.
- HUNGARNET
- SUNET https://wiki.sunet.se/pages/viewpage.action?pageId=30441624.
- SURFNET: https://www.surf.nl/en/surfwireless-wifi-as-a-service
- Uninett

GÉANT
Networks • Services • People

Thank you

Any questions?

www.geant.org

© GÉANT Association on behalf of the GN4 Phase 3 project (GN4-3).
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).