**HLD & LLD Design of Internet Service Provider**

**1) Introduction**

The purpose of this document is to provide valid information for the constituent members including Low-level Design and High-Level design in a concise overview of a large geographical area service within the framework of the bill and compliance with IEEE Standards.

The framework of the research of the project and its development should be strictly adhered to in order to create reliable forms of services and also to connect with other geographical parts. The main vision of service and support of our fellow human beings but also of their dreams through our services, making them possible.

The "corporate" network will bring the so-called Industry Standards from reliable products in this list for its foundation and its spread within them the direct support and creation of a company-consumer bond

The final creation of the network topology will be fully functional and scalable as its effectiveness has been repeatedly certified in laboratory-controlled environments.

The physical existence of the network trunk will be completed in a 2-phase schedule. Installations and network supply with the physical placement of trunk network devices in specific locations as pre-decided with techniques for creating uninterrupted operation of 2 level DWDM devices

Immediately after this phase, the physical interconnection of these devices will take place as they will then be manageable and modifiable by specialized engineers through special software.

**2) Network Product Overview**

The network will consist of industry Standards & IEEE compatible hardware multi-Service Switches L3, Edge routers designed to deliver uninterrupted operation, high efficiency and reliability CIA (confidentiality, integrity, availability) according to the plan of the Service Provisioning network with the goal and vision of immediate response to fluctuating demands but also failure. Services with full QoS application-level awareness and consumer awareness and evolving through preferential control for new revenue streams.

The main part of the network backbone will be subdivided into 3 other networks that will each be for Mobile - telephony, fixed, security - supply - content (CDN)

There will be an Edge Router in each geographical county that will register subscribers based on IP’s Legal Ownership from IANA as decided in the respective BRAS-Next gen (BNG)

Due to technological transfer full existence and support Ipv4 + Ipv6 Islands for technological compromise. Separation packages simply or operationally and advanced business technical support through communication applying IP MPLS L3 Vpn, SDN, ISDN.

The network will manage both external subscribers and employees via VPN, Cloud Solutions, Active Directories, logs.

An intranet which will have managements in each building Urban Center with at least 128 stations for employees per business floor.

3 tier Access, Aggregation / Distribution, Data Center Core (IP / FCoE + SAN Network).

**Access Layer**

(Access Control)

1)802.1x NAC/CCA Mac auth Bypass

2)Web-Based Proxy Auth

3)PPPxx

**Distribution Layer**

(path isolation)

1. Vlan/.1Q
2. GRE DMVPN
3. VRF-Lite
4. MPLS
5. ACL

**Data Center Core**

(policy enforcement)

Firewall, Context (CSM ACE)

Policy Management

These decisions were made in accordance with the Lifecycle Ecosystem ITIL development plan

Service Strategy, Service Design, Service Transition, Service Operation, Continual Process improvement (Prepare-Plan-Design-Implement-operate-Optimize)

**3) Network Detail Overview**

The network will consist of ipv4 and ipv6 protocols. Specifically, ipv6 networks with prefix 2001: 1111: 2222: 3333 :: / 64 and ipv4 networks with prefix 192.168.1.0/24 with 128 IP’s minimum will be given

on each floor of the HQ store.

Ipv6 will be used for customer service but also the service of employees in internal networks per urban centre (store). There will also be 2 stores in the HQ number.

In the rest of the stores, the connection will be made through Active Directories and the employees will be given access through CDN Firewall. So the operating system will be Windows Server.

Of course, all transactions will be recorded automatically on a Log Server. This will also increase the security of the information system in case of malicious action.

Following the service of the company's requirements, VLANs with subnet / 29 will be needed.

These will be used to connect database servers, printers, file servers and mail servers.

A very important implementation of the requirement will clearly be the remote management of the servers as well as the terminals of each employee. This can be done by setting up a Vpn Server.

Wi-Fi is also a very important part of the requirements. It will belong to a separate VLAN with subnet / 29. That is 255,255,255,248. This includes Wi-Fi portals. For customer service as well as employees.

Wi-Fi networks will be an open system so users can connect without a key.

For security reasons, however, the authentication will be done by a portal. Clearly, within the portal, there will be an indication that "in case of malicious action I take full responsibility".

This will help the business not to be exposed to malicious actions of a user. Finally, the movements will be recorded in the Log Server.

The wiring to implement the above will be the so-called structured wiring vertically and horizontally.

This will be implemented with MDF / IDF. That is, in essence, racks/cabinets for switches.

On each floor, there will be a closet with IDF where the copper will be connected to the central MDF and again with copper the employees will be connected to the core of the company in the main HQ.

Of course, fiber optics can not be missing. They will be used for customer package upgrades. Resulting in very high downloading / uploading and streaming speeds.

The topologies that will be used for all of this will be a mix of ring and star topologies.

**4) Functionality Software/Hardware**

Blade servers will mainly use multi-rack modular design data centres.

With all safety standards both physical and technological.

Thanks to the extreme blade servers modular the provision of services can be done in large geographical departments and line cards.

Of course for continuous service, the blade servers must be active-standby.

This means that if one card breaks on the cisco machine, the other takes over automatically.

With these machines, the bar rises and we now provide specifications (CIA) that is confidentiality, integrity, availability.

This is achieved through service production and delivery with the ultimate goal and vision of evolution and continuous movement of services in virtualization and cloud solution of the Private cloud.

1. **Functionality and possibilities of Network**

* **Switch layer 3:** Switch layer 3 combines the functionality of a switch and router, combines devices located on the same subnet. It can support routing protocols, control incoming packets, and make routing decisions based on source and destination addresses. The advantages of switch layer 3 in our company are:

**1)** Lower network latency as a package does not need to do additional extra hops from a router

**2)** Simpler troubleshooting

**3)** Facilitates the configuration process for VLANs, no router is needed between each VLAN.

* **Edge router:** It is a specialized router that allows an internal network to connect to external networks.
* **GRE:** Tunneling protocol by Cisco Systems, integrates a wide variety of network layer protocols into virtual point-to-point or multipoint links of an Internet protocol network.
* **DMVPN:** Dynamic tunnelling VPN network to avoid the need for pre-configure (static) all possible end-point peers, including IPsec (Internet Protocol Security) and ISAKMP (Internet Security Association and Key Management Protocol).
* **VRF:** It is a technology that allows multiple instances of a routing table to coexist on the same router at the same time. With VRFs, where TCP / IP layer 3 is VLAN, network performance is improved because network paths can be segmented without the need for multiple routers.
* **MPLS:** MPLS can integrate packages of various protocols, supports a number of access technologies such as T1 / E1, ATM, Frame, Relay and DSL. It also allows our network data packets to be labelled and decisions to promote them are made solely on the content of that tag, without the need to consider the packet itself.
* **ACL:** Access Control Lists are a set of rules that dictate which computers on the network will have access to which particular service. ACLs have network routers and various servers.

1. **Discuss about possible security issues**

The security of the information system in our company is very important so that it can function properly and reliably. For this reason, there must be proper planning of security and safety policy. A key pillar of information security is the CIA triad model which is designed to guide the organization's security policy. The confidentiality, integrity and availability of information should therefore be ensured.

Confidentiality measures are designed to prevent sensitive information from being alerted to the wrong people while ensuring that authorized people can access it. The data should be categorized according to how important it is and appropriate security measures should be taken.

Integrity ensures that the data will not be altered by unauthorized persons.

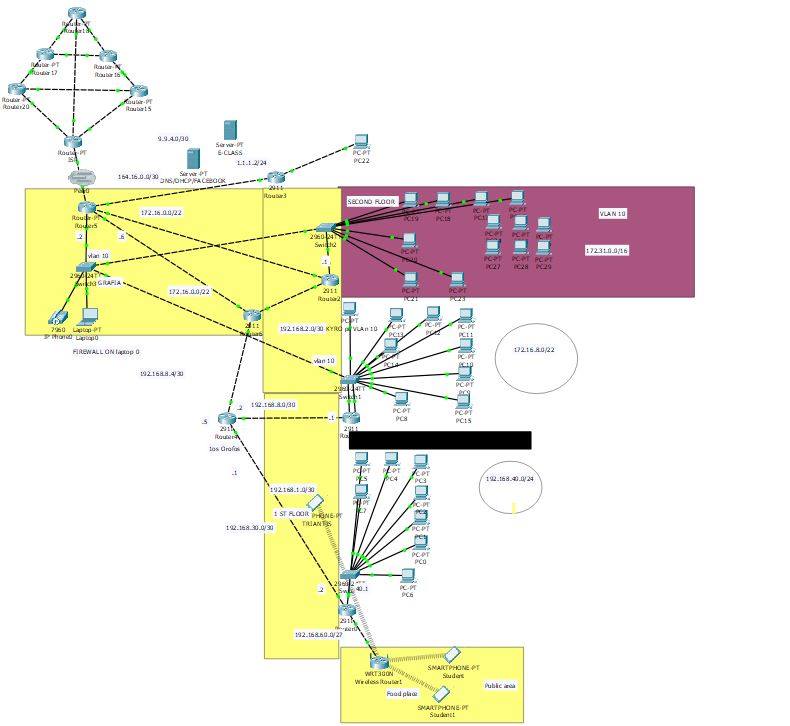
Availability ensures that data and system resources (computers, networks) will be available to users whenever their use is required.

The possible security problems that may arise in the company can be divided into two levels.

**Physical level:** This level contains the security that has to do with the protection of the equipment and the personnel of the company. Initially, there should be control of the access of the people who enter the company. This is achieved by using the Access Control System where each employee must have their own RFID card in order to record the people entering and leaving the company. Also, there should be security cameras on the premises of the building without violating the GDPR. In this way, a better identification is made of the person who enters the company. There should also be fire detection and fire extinguishing system installed, as well as fire extinguishers in the various areas of the building. Particular emphasis is given to server rooms where the fire extinguishing system will be nitrogen and not water so that there is no further damage to the server rooms.

**Network security:** Below is various attacks that can occur in a network and how they can be dealt with.

* **ARP Poisoning:** Static ARP Entries + ARP spoofing detection and prevention software.
* **A distributed Denial-of-service attack (DDoS):** Black holing + more bandwidth.
* **Smurf attack:** Use antivirus and anti-malware protection + disable IP broadcast address on each router, as well as configure hosts and routers not to respond to ICPM echo requests.
* **Broadcast Storm:** Use VLANs + limit the amount of data a port can take.
* **MAC flooding:** Cisco switches are equipped with a built-in security feature against mac flooding attacks, called Port Security.
* **IP spoofing:** Use a firewall that rejects all packets that reach the incoming side of the firewall, where the source IP corresponds to one of the internal IPs.
* **Man-in-the-Middle attack:** VPN, HTTPS, continuous control of public key pair authentication, strong WPA2 encryption at the access point.
* **SQL Injection:** HTTPS + avoid using dynamic queries in applications.
* **Phishing attack:** Anti-phishing software + continuous information and training of employees to prevent cyber-fishing and generally in social engineering attacks.



The image represents an HQ part as it does not fully comply with the content of the text.

**CREATED BY**

**MICHAIL MARKOU + MANIOS ATHANASIOS + GIANNIS CHAIDOS**