Piraeus Port Authority S.A.
Procurement Department
10, Akti Miaouli,
GR 185 38,
Piraeus, Greece.
tel: +30 210 4550189
fax: +30 210 4550187
e-mail: procurement@olp.gr

Subject: Clarifications to the interested parties regarding the Call of Tender **FOR THE AWARD OF PROCUREMENT IT EQUIPMENT REPLACEMENT PROGRAM – FIRST PERIOD NETWORK EQUIPMENT**

1. Security

1.1 Campus & DC Firewalls

1.7 Proposed devices must have dual Main Control Boards for HA: Please change the specification to 'Security Modules' as Control Plane redundancy will be achieved with Active/Active or Active/Standby function.

The consolidation of Data Center and Campus Network security services require high levels of availability. Hence, box level control plane redundancy considered as mandatory requirement.

1.11 Required minimum IPS performance ≥ 34 Gbps: Please change the specification as this is way above current equipment specifications (Cisco ASA 5540 and Cisco Catalyst 6500 FWSM) and drives to more than 500% expansion and unnecessary costs. Please include and traffic analysis and performance needs forecast studies that lead to this specification.

We were unable to identify any technical standing behind your comment as well as your calculations. The new design imposes many changes over the current design, including the Data Center and Campus network. It is a centralized approach where many resources reside either in our Data Center onsite or offsite, in a Disaster Data Center. The main driver behind the centralization is the Virtualization on DC Resources, User Endpoints and services that are related to User Endpoints requiring split second resiliency, end to end network visibility and lower contention ratios (i.e. increased per user bandwidth).

Being able to quickly and securely interconnect with corporate networks abroad is another factor on introducing consolidated Campus & Data Center Security services in the network. Hence, the need for elevated requirements on IPS function performance.

1.12 Required minimum FW performance IPv4/IPv6 (IMIX) ≥ 68 Gbps /≥ 68 Gbps: Please remove this specification because a Legacy Stateful Firewall is not an adequate security measure, can be replaced by features in switches and routers that are of lower cost and considering modern threats, there must be nothing less than a NGFW in an organization. Alternative, change the specification as this is way above current equipment specifications (Cisco ASA 5540 and Cisco Catalyst 6500 FWSM) and drives to more than 1000% expansion and unnecessary costs. Please include and traffic analysis and performance needs forecast studies that lead to this specification.

We were unable to identify any technical standing behind your comment. This requirement is one of industry standard indicators of measuring the performance of the Firewalling function either as a standalone device or in the form of a Next Generation Firewall.

The new design imposes many changes over the current design, including the Data Center and Campus network. It is a centralized approach where many resources reside either in our Data Center onsite or offsite, in a Disaster Data Center. The main driver behind the centralization is the Virtualization on DC Resources, User Endpoints and services that are related to User Endpoints requiring split second resiliency, end to end network visibility and lower contention ratios (i.e. increased per user bandwidth).

Being able to quickly and securely interconnect with corporate networks abroad is another factor on introducing consolidated Campus & Data Center Security services in the network. Hence, the need for elevated requirements on Firewall function performance.

1.13 Required minimum number of Concurrent Firewall Connections ≥ 68 Million: Please remove this specification because the number of connections is not an indicator of performance, do not adhere to all services (IPS, Antimalware etc) and points to specific vendors and models. Please include and traffic analysis and performance needs forecast studies that lead to this specification.

We were unable to identify any technical standing behind your comment. This requirement is one of industry standard indicators of measuring the performance of the Firewall function of a Next Generation Firewall. Please refer to the last paragraph of the answer # 1.12 for the reasons that led to this specification.

1.14 Number of New Connections Per Second ≥ 1 Million: Please remove this specification because number of connections are not an indicator of performance, do not adhere to all services (IPS, Antimalware etc) and points to specific vendors and models. Please include and traffic analysis and performance needs forecast studies that lead to this specification.

We were unable to identify any technical standing behind your comment. This requirement is one of industry standard indicators of measuring the performance of the Firewall function of a Next Generation Firewall. Please refer to the last paragraph of the answer # 1.12 for the reasons that led to this specification.

1.18 Proposed devices must support Virtual Firewalls: Please remove this specification because there is no current stated use of virtual firewalls or future need indicated in the tender.

We were unable to identify any technical standing behind your comment. This requirement is mandatory given design's foundational requirements. The DC & Campus security services will be consolidated in to a pair of NGFW boxes. The DC security services will run on a separate Virtual Firewall (Virtual Context) while the Campus Security services will run on separate Virtual Firewall (Virtual Context).

1.19 Number of Virtual Firewall licenses needed upon the delivery of the equipment ≥ 10: Please remove this specification because there is no current stated use of virtual firewalls or future need indicated in the tender.

We were unable to identify any technical standing behind your comment. This requirement is mandatory given design's foundational requirements. The DC & Campus security services will be consolidated in to a pair of NGFW boxes. The DC Security services will run on a separate Virtual Firewall (Virtual Context) while the Campus Security services will run on separate Virtual Firewall (Virtual Context). The remaining number of Virtual Firewall licenses (Virtual Context licenses) will be utilized in the future to cover already identified and recorded security service needs on subsystems / interconnections, indicatively:

- **Real-time Communication services**
- **Interconnections with other intranets abroad**
- **SIP trunk based packet voice services**
- **Physical Security Services infrastructure (i.e. Access Control, CCTV, etc)**
- **"Smart Port" applications**

1.20 Proposed equipment must support security function virtualization: Security feature, forwarding, user virtualization, management, virtualization, views, and resources (such as bandwidth and session): Please remove this specification because there is no current stated use of it or future need indicated in the tender. Also, it is overlapping with specification 1.18 and 1.19.

We were unable to identify any technical standing behind your comment. This requirement is related to NGFW Virtual Firewalls (Virtual Contexts). Please refer to answers given to #1.18 and #1.19 for further information.

1.21 The proposed equipment must support resource quota management: Ability to limit the number of resources for a virtual firewall restrict the maximum and minimum values. Resources must include the number of sessions, bandwidth usage, number of unified policies, such as the security policy, traffic limiting policies, NAT policies, and policy-based routing), and local user (group): Please remove this specification because there is no current stated use of virtual firewalls or future need indicated in the tender.

We were unable to identify any technical standing behind your comment. This requirement is mandatory given design's foundational requirements. Please refer to the answers given to #1.18, #1.19 and #1.20 for further information.

1.28 Supports multiple user authentication methods, including local, RADIUS, TACACS or equivalent, SecurID, AD, CA, LDAP, and Endpoint Security: Please change this specification to 'including local, RADIUS, TACACS or equivalent, AD, LDAP and optionally SecurID, CA and Endpoint Security' because all methods are not supported by the majority of vendors and lead to vendor-specific references.

Comment accepted.

1.35 Supports IPv4 static routes, policy-based routing, routing policies, multicast, RIP, OSPF, BGP, and IS-IS: Please remove RIP and IS-IS as there are not commonly used protocols in security devices and not recommended by most vendors. Also, this specification points to specific vendors and models.

The requirement modified as follows: "Supports IPv4 static routes, policy-based routing, routing policies, multicast, OSPF, BGP and optionally, IS-IS and RIP.

For your information, there many vendors in the industry supporting this functionality.

1.36 Supports IPv6 static routes, policy-based routing, routing policies, RIPng, OSPFv3, BGP4+,and IPv6 IS-IS: Please remove RIPng and IS-IS as there are not commonly used protocols in security devices and not recommended by most vendors. Also, this specification point to specific vendors and models.

The requirement modified as follows: "Supports IPv6 static routes, policy-based routing, routing policies, OSPFv3, BGP4+ and optionally, IPv6 IS-IS and RIPng.

For your information, there many vendors in the industry supporting this functionality.

1.38 Supports data leak prevention to identify and filter files and content (different types of information, such as ID cards, credit cards, debit cards, social security cards etc) in transit: Please remove this specification because Data Leak Prevention is a security technology that is offered by separate products and points to specific vendors and models.

Comment accepted. The requirement changed from mandatory to optional.

1.39 Supports multiple highly reliable VPN features, such as IPsec VPN, SSL VPN, L2TP VPN, DSVPN or equivalent, and GRE: Please remove this specification because the Data Center firewall is not an edge VPN device and VPN terminating from external organizations are a security risk. Alternatively, please change to 'and optionally L2TP VPN, DSVPN or equivalent and GRE**'** because these are not commonly used protocols in security devices and not recommended by most vendors. Also, this specification point to specific vendors and models. Please allow to offer separate device or devices to fulfil this specification.

The requirement modified as follows:
"Supports multiple highly reliable VPN features, such as IPsec VPN, SSL VPN, GRE/L2TP VPN, DMVPN/DSVPN or equivalent"

We were unable to identify any technical standing behind your comment. The new design will have the DC and the Campus security services consolidated in a pair of High End NGFW. The VPN features are required for cases where interconnection with other corporate networks or subsidiaries is needed. The data will be traversing connectivity provider's network unencrypted hence, the need for encryption.

For your information, there many vendors in the industry supporting this functionality.

This functionality will help us to achieve a secure WAN infrastructure. Hence, this functionality is mandatory.

This functionality can be offered either as an integrated function or as a separate solution, following the redundancy guidelines as required for the DC & Campus

NGFW"

1.41 Allows users to create and manage virtual security services, including firewall, intrusion prevention, and antivirus services, on the same physical device: Please remove this specification because there is no current stated use of it or future need indicated in the tender. Also, it is overlapping with specification 1.18, 1.19 and 1.21.

We were unable to identify any technical standing behind your comment. This functionality is mandatory. Please refer to answers #1.18, #1.19 and #1.20 for further details.

1.43 Proposed equipment must support CGN functions including: NAT444, PCP and NAT64 to ease connectivity to other corporate intranets worldwide: Please remove this specification because the Data Center firewall is not a carrier-grade NAT devices use to perform large scale NAT operations. Also, this specification point to specific vendors and models. Please allow to offer separate device or devices to fulfil this specification.

The requirement modified as follows:
"Proposed equipment must support large scale NAT functions including: NAT444, NAT64 and optionally PCP to ease connectivity to other corporate intranets worldwide"

We were unable to identify any technical standing behind your comment. Please note that, we are not looking for a security solution which will handle only DC specific security tasks. The design requirements consolidate the Data Center and Campus Security Services in a pair of high end NGFWs. This functionality is mandatory.

For your information, there many vendors in the industry supporting this functionality.

You are allowed to offer separate devices to fulfill this specification by following the redundancy guidelines as required for the DC & Campus NGFW.

1.2 External Firewalls

1.11 Supports multiple user authentication methods, including local, RADIUS TACACS, SecurID, AD, CA, LDAP, and Endpoint Security: Please change this specification to ‘including local, RADIUS, TACACS or equivalent, AD, LDAP and optionally SecurID, CA and Endpoint Security’ because all methods are not supported by the majority of vendors and lead to vendor-specific references.

Comment accepted. The requirement modified as follows: “including local, RADIUS, TACACS or equivalent, AD, LDAP and optionally, SecurID, CA and Endpoint Security”

1.17 VPN throughput AES per device ≥ 5 Gbps: Please change this specification to ‘VPN throughput AES per device ≥ 5 Gbps ’ as there are currently not enough edge connections (Internet/MPLS/etc) to cover 5Gbps and this throughput is not attainable by business standards and this country’s telco line speeds.

We were unable to identify what is the suggested change. Our country has a steady growth rate on F/O based access capacities according to a number of publicly available reports from the EU and OECD. Consequently, since one of the foundational design guidelines is to build a future proof infrastructure, this functionality is considered mandatory.

1.20 Maximum Concurrent Connections ≥ 5M: Please remove this specification because number of connections are not an indicator of performance, do not adhere to all services (IPS, Antimalware etc) and points to specific vendors and models. Please include and traffic analysis and performance needs forecast studies that lead to this specification.

We were unable to identify any technical standing behind your comment. This requirement is one of industry standard indicators of measuring the performance of the Firewalling function either running as a standalone device or in the form of a Next Generation Firewall. There many vendors in the industry able to attain this level of performance.

1.21 Connections Per Second ≥ 100K: Please remove this specification because number of connections are not an indicator of performance, do not adhere to all services (IPS, Antimalware etc) and points to specific vendors and models. Please include and traffic analysis and performance needs forecast studies that lead to this specification.

We were unable to identify any technical standing behind your comment. . This requirement is one of industry standard indicators of measuring the performance of the Firewalling function either running as a standalone device or in the form of a Next Generation Firewall. There many vendors in the industry able to attain this level of performance.

1.34 Capacity per Hard Disk ≥ 500GB: Please remove this specification because disk size does not adhere to any performance metric. Please include and traffic analysis and performance needs forecast studies that lead to this specification.

This specification is required for local storage of logs and reports. The requirement modified as follows: "Local storage of logs and reports without using the NVRAM. Required minimum storage capacity ≥ 240GB"

1.35 Supports IPv4 static routes, policy-based routing, routing policies, multicast, RIP, OSPF, BGP, and IS-IS: Please remove RIP and IS-IS as there are not commonly used protocols in security devices and not recommended by most vendors. Also, this specification points to specific vendors and models.

The requirement modified as follows: "Supports IPv4 static routes, policy-based routing, routing policies, multicast, OSPF, BGP and optionally, IS-IS and RIP.

There many vendors in the industry supporting this functionality.

1.36 Supports IPv6 static routes, policy-based routing, routing policies, RIPng, OSPFv3, BGP4+,and IPv6 IS-IS: Please remove RIPng and IS-IS as there are not commonly used protocols in security devices and not recommended by most vendors. Also, this specification point to specific vendors and models.

The requirement modified as follows: "Supports IPv6 static routes, policy-based routing, routing policies, OSPFv3, BGP4+ and optionally, IPv6 IS-IS and RIPng.

There many vendors in the industry supporting this functionality.

1.38 Supports data leak prevention to identify and filter files and content (different types of information, such as ID cards, credit cards, debit cards, social security cards etc) in transit: Please remove this specification because Data Leak Prevention is a security technology that is offered by separate products and points to specific vendors and models.

Comment accepted. The requirement changed from mandatory to optional.

1.39 Supports multiple highly reliable VPN features, such as IPsec VPN, SSL VPN, L2TP VPN, DSVPN or equivalent ,and GRE: Please remove this specification because the Edge firewall is not a VPN device and VPN terminating from external organizations should be on a dedicated VPN concentrator/gateway secured in a separate zone. Alternatively, please change to '<u>and optionally L2TP VPN, DSVPN or equivalent and GRE</u>' because these are not commonly used protocols in security devices and not recommended by most vendors. Also, this specification point to specific vendors and models. Please allow to offer separate device or devices to fulfil this specification.

The requirement modified as follows:
"Supports multiple highly reliable VPN features, such as IPsec VPN, SSL VPN, GRE/L2TP VPN, DMVPN/DSVPN or equivalent"

We were unable to identify any technical standing behind your comment. Project's requirements on terminating remote, Internet based VPN users is limited. To date, there are around 75 remote users using this service. These sizing figures are considered way too small in order for us to request a dedicated VPN concentration device. This also explains the requirement why we need Virtual Contexts.

You are allowed to offer a dedicated set of VPN concentrators following the high availability guidelines of the Internet Firewalls.

There are many vendors in the industry supporting this functionality built in to their products.

1.40 Offered with licenses for remote access SSL VPN of at least 100 concurrent connections: Please remove this specification because the Edge firewall is not a VPN device and VPN terminating from external users should be on a dedicated VPN concentrator/gateway secured in a separate zone. Also, this specification point to specific vendors and models. Please allow to offer separate device or devices to fulfil this specification.

This requirement is mandatory. Please refer to answer #1.39. There are many vendors in the industry supporting this functionality built in to their products.

1.41 Supports application-layer protocol-based traffic control policies, including setting the maximum bandwidth, guaranteed bandwidth, and protocol traffic priority: Please change this specification to 'including setting the maximum bandwidth and optionally guaranteed bandwidth, and protocol traffic priority' because all methods are not supported by the majority of vendors and lead to vendor-specific references.

Comment accepted. There are many vendors in the industry supporting this functionality built in to their products.

1.42 Allows users to create and manage virtual security services, including firewall, intrusion prevention, and antivirus services, on the same physical device: Please remove this specification because there is no current stated use of it or future need indicated in the tender and points to specific vendors and models.

We were unable to identify any technical standing behind your comment. Please refer to answer #1.39. This requirement is mandatory. There are many vendors in the industry supporting this functionality.

1.43 Supports intelligently selecting carrier links based on destination IP addresses; supports active/standby interface configuration and load balancing by percentage: Please remove this specification because this features is offered be specialized devices and points to specific vendors and models. Please allow to offer separate device or devices to fulfil this specification.

This requirement is mandatory. You are allowed to offer a dedicated set of devices to fulfill this requirement following the high availability guidelines of the Internet Firewalls.

3.4 Submission of Offers. ”Please allow us enough days to receive your response and submit our proposal by granting at least a 2 week extension of the final submission date.”

The final submission date of the offers cannot be extended.

2. Switches

2.1 DC Switches

4.24 Proposed equipment must support REP (Resilient Ethernet Protocol), SEP (Smart Ethernet Protection) or any equivalent ring protocol, which can support less than 50ms failover time

Please remove this specification because this features concerns ring topologies, which are irrelevant to the project, and add extra costs.

The requirement changed from mandatory to optional.

8.5 Proposed equipment must support multi domain authentication from a single physical port so that the interconnected devices (for instance: IP Telephone and Workstation) can be dynamically assigned to their respective service VLAN

Please remove this specification because it is irrelevant to the core switches (refers to access ones).

The requirement changed from mandatory to optional. Consequently, the requirement #8.6 is also changed to optional.

2.2 K6-K8 Campus Core Switches

1.4 Frame suitable for fitting in to a 19" rack, 600mm depth

Please modify the specification to "Frame suitable for fitting in to a 19" rack, 800mm depth" to allow equipment with greater depth.

Comment Accepted. The specification changed as follows:

"1.4 Frame suitable for fitting in to a 19" rack, 800mm depth"

2. K8 Campus Core

Please remove the following part of the compliance table

1.7	Main Control Board RAM	≥ 8 GB
1.8	Main Control Board Flash	≥ 4 GB

1.9	Number of Line Card Slots	≥ 4
1.10	Per slot bandwidth	≥ 440 Gbps
1.11	Switching Capacity	≥ 4 Tbps
1.12	Backplane Capacity	≥ 20 Tbps
1.13	Forwarding Rate	≥ 6000 Mpps
1.14	FIB Entries	≥ 2 Million

and replace it with something simpler like

1.7	Main Control Board or supervisor RAM	≥ 8 GB
1.8	Main Control Board or supervisor Flash	≥ 2 GB
1.9	Number of Line Card Slots	≥ 4
1.10	Per slot bandwidth	≥ 440 Gbps
1.11	Max Local Switching Capacity	≥ 1 Tbps
1.12	System forwarding Capacity	≥ 20 Tbps
1.13	Forwarding Rate	≥ 6000 Mpps
1.14	FIB Entries	≥ 2 Million

in order to conclude as many vendors as possible being able to contribute to the solution.

We were unable to identify any technical standing behind your comment on "simplicity". There are no changes accepted in the table.

The requirements that are requested to be removed (Forwarding Rate, FIB Entries) are industry standard technical specifications directly related to the scalability of the required equipment. You're allowed to respond with your own figures.

4.5 Proposed equipment must support VLAN-based, 802.1p-based, and MQC based VLAN mapping

Please remove MQC requirement as it refers to specific vendor.

We were unable to identify any technical standing behind your comment. MQC is a generic term used by many vendors and it stands for "Modular Quality of Service (QoS) Command-Line Interface"

4.8 Proposed equipment must support local and remote port mirroring:

- **MQC Based**
- **ACL Based**

Please remove MQC requirement as it refers to specific vendor.

We were unable to identify any technical standing behind your comment. MQC is a generic term used by many vendors and it stands for "Modular Quality of Service (QoS) Command-Line Interface"

8.5 Proposed equipment must support multi domain authentication from a single physical port so that the interconnected devices (for instance: IP Telephone and Workstation) can be dynamically assigned to their respective service VLAN

Please remove this specification because it is irrelevant to the core switches, (refers to access ones).

The requirement changed from mandatory to optional. Consequently, the requirement for #8.6 is also changed to optional.

9.6 Proposed equipment must support OAM discovery, errored symbol period events, errored frame events, errored frame seconds summary events, fault advertisement, and remote loopback as per IEEE 802.3ah-2004 EFM

Please remove this specification because it is irrelevant to the core switches, (refers to last mile Service Provider networks).

We were unable to identify any technical standing behind your comment. This requirement is an industry standard way of monitoring end to end Ethernet network performance.

3. DMZ Switches

1.8 Number of built-in QSFP+ Ports ≥ 2

1.9 One Expansion slot for additional QSFP+ ports ≥ 4

(Per DMZ Switch Requirement)

Please accept solution that offers 6 QSFP+ fixed ports

You are allowed to offer a solution with 4 QSFP+ ports minimum. These ports must support stacking by back to back connections between the DMZ switches. Stacking by using dedicated stack ports is also accepted. Part of the QSFP+ ports will be used as uplink ports facing towards the Core Nodes, while the others, for stack interconnect. The stack members will either be collocated or optimally, will be installed in separate places to achieve geographical redundancy.

With the change on the minimum allowed number of required 40GbE ports, the requirement #1.2 Forwarding Performance changed to 350 Mpps.

4.5 Proposed equipment must support VLAN-based, 802.1p-based, and MQCbased VLAN mapping

4.9 Proposed equipment must support local and remote port mirroring:

- **MQC Based**
- **ACL Based**

Please remove MQC requirement as it refers to specific vendor.

We were unable to identify any technical standing behind your comment. MQC is a generic term commonly used by many vendors and it stands for "Modular Quality of Service (QoS) Command-Line Interface"

4.18 Proposed equipment must support REP (Resilient Ethernet Protocol), SEP (Smart Ethernet Protection) or any equivalent ring protocol which can support less than 50ms failover time

Please remove this specification because this features concerns ring topologies, which are irrelevant to the project, and add extra costs.

This requirement concerns "segment" topologies. It is included to add flexibility in cases like ours, when the number of available F/O cabling is limited.

9.8 Proposed equipment must support OAM discovery, errored symbol period events, errored frame events, errored frame seconds summary events, fault advertisement, and remote loopback as per IEEE 802.3ah-2004 EFM

Please remove this specification because it is irrelevant to the core switches, (refers to last mile Service Provider networks).

We were unable to identify any technical standing behind your comment. This requirement is an industry standard way of monitoring end to end Ethernet network performance. This is required for the DMZ switches.

9.7 Proposed equipment must support Alarm Indication Signal (AIS) and delay measurement (DM) as per ITU-T Y.1731

Please remove this specification because it is irrelevant to the core switches, (refers to Service Provider networks).

The requirement changed from mandatory to optional. This is required for the DMZ switches.

4. K2HQ - Campus Aggregation

1.8 Number of built-in QSFP+ Ports ≥ 2

1.9 One Expansion slot for additional QSFP+ ports ≥ 4

(Per DMZ Switch Requirement)

Please accept solution that offers 6 QSFP+ fixed ports

You are allowed to offer a solution with 4 QSFP+ ports minimum. These ports must support stacking by back to back connections between the Aggregation switches. Stacking by using dedicated stack ports is also accepted. Part of the QSFP+ ports will be used as uplink ports facing towards the Core Nodes, while the others, for stack interconnect. The stack members will be collocated.

4.5 Proposed equipment must support VLAN-based, 802.1p-based, and MQC based VLAN mapping

4.9 Proposed equipment must support local and remote port mirroring:

- **MQC Based**
- **ACL Based**

Please remove MQC requirement as it refers to specific vendor.

We were unable to identify any technical standing behind your comment. MQC is a generic term commonly used by many vendors and it stands for "Modular Quality of Service (QoS) Command-Line Interface"

4.18 Proposed equipment must support REP (Resilient Ethernet Protocol), SEP (Smart Ethernet Protection) or any equivalent ring protocol which can support less

than 50ms failover time

Please remove this specification because this features concerns ring topologies, which are irrelevant to the project, and add extra costs.

This requirement concerns "segment" topologies. It is included to add flexibility in cases like ours, when the number of available F/O cabling is limited or difficult to be laid.

9.8 Proposed equipment must support OAM discovery, errored symbol period events, errored frame events, errored frame seconds summary events, fault advertisement, and remote loopback as per IEEE 802.3ah-2004 EFM

Please remove this specification because it is irrelevant to the core switches, (refers to last mile Service Provider networks).

We were unable to identify any technical standing behind your comment. This requirement is an industry standard way of monitoring end to end Ethernet network performance. This is required for the Campus Aggregation switches.

9.7 Proposed equipment must support Alarm Indication Signal (AIS) and delay measurement (DM) as per ITU-T Y.1731

Please remove this specification because it is irrelevant to the core switches, (refers to Service Provider networks).

The requirement changed from mandatory to optional. This is required for the Aggregation switches.

5. K8 - Campus Aggregation

1.8 Number of built-in QSFP+ Ports ≥ 2

1.9 One Expansion slot for additional QSFP+ ports ≥ 4

(Per DMZ Switch Requirement)

Please accept solution that offers 6 QSFP+ fixed ports

You are allowed to offer a solution with 4 QSFP+ ports minimum. These ports must support stacking by back to back connections between the Aggregation switches. Stacking by using dedicated stack ports is also accepted. Part of the QSFP+ ports will be used as uplink ports facing towards the Core Nodes, while the others, for stack interconnect. The stack members will be collocated.

With the change on the minimum allowed number of required 40GbE ports, the

requirement #1.2 Forwarding Performance changed to 350 Mpps.

4.5 Proposed equipment must support VLAN-based, 802.1p-based, and MQCbased VLAN mapping

4.9 Proposed equipment must support local and remote port mirroring:

- **MQC Based**
- **ACL Based**

Please remove MQC requirement as it refers to specific vendor.

We were unable to identify any technical standing behind your comment. MQC is a generic term commonly used by many vendors and it stands for "Modular Quality of Service (QoS) Command-Line Interface"

4.18 Proposed equipment must support REP (Resilient Ethernet Protocol), SEP (Smart Ethernet Protection) or any equivalent ring protocol which can support less than 50ms failover time

Please remove this specification because this features concerns ring topologies, which are irrelevant to the project, and add extra costs.

This requirement concerns "segment" topologies. It is included to add flexibility in cases like ours, when the number of available F/O cabling is limited.

9.8 Proposed equipment must support OAM discovery, errored symbol period events, errored frame events, errored frame seconds summary events, fault advertisement, and remote loopback as per IEEE 802.3ah-2004 EFM

Please remove this specification because it is irrelevant to the core switches, (refers to last mile Service Provider networks).

We were unable to identify any technical standing behind your comment. This requirement is an industry standard way of monitoring end to end Ethernet network performance. This is required for the Campus Aggregation switches.

9.7 Proposed equipment must support Alarm Indication Signal (AIS) and delay measurement (DM) as per ITU-T Y.1731

Please remove this specification because it is irrelevant to the core switches, (refers to Service Provider networks).

The requirement changed from mandatory to optional. This is required for the Campus Aggregation switches.

6. K21 - Campus Aggregation

1.8 Number of built-in QSFP+ Ports ≥ 2

1.9 One Expansion slot for additional QSFP+ ports ≥ 4

(Per DMZ Switch Requirement)

Please accept solution that offers 6 QSFP+ fixed ports

You are allowed to offer a solution with 4 QSFP+ ports minimum. These ports must support stacking by back to back connections between the Aggregation switches. Stacking by using dedicated stack ports is also accepted. Part of the QSFP+ ports will be used as uplink ports facing towards the Core Nodes, while the others, for stack interconnect. The stack members will be collocated.

With the change on the minimum allowed number of required 40GbE ports, the requirement #1.2 Forwarding Performance changed to 350 Mpps.

4.5 Proposed equipment must support VLAN-based, 802.1p-based, and MQCbased VLAN mapping

4.9 Proposed equipment must support local and remote port mirroring:

- **MQC Based**
- **ACL Based**

Please remove MQC requirement as it refers to specific vendor.

We were unable to identify any technical standing behind your comment. MQC is a generic term commonly used by many vendors and it stands for "Modular Quality of Service (QoS) Command-Line Interface"

4.18 Proposed equipment must support REP (Resilient Ethernet Protocol), SEP (Smart Ethernet Protection) or any equivalent ring protocol which can support less than 50ms failover time

Please remove this specification because this features concerns ring topologies, which are irrelevant to the project, and add extra costs.

This requirement concerns "segment" topologies. It is included to add flexibility in

cases like ours, when the number of available F/O cabling is limited.

9.8 Proposed equipment must support OAM discovery, errored symbol period events, errored frame events, errored frame seconds summary events, fault advertisement, and remote loopback as per IEEE 802.3ah-2004 EFM

Please remove this specification because it is irrelevant to the core switches, (refers to last mile Service Provider networks).

We were unable to identify any technical standing behind your comment. This requirement is an industry standard way of monitoring end to end Ethernet network performance. This is required for the Campus Aggregation switches.

9.7 Proposed equipment must support Alarm Indication Signal (AIS) and delay measurement (DM) as per ITU-T Y.1731

Please remove this specification because it is irrelevant to the core switches, (refers to Service Provider networks).

The requirement changed from mandatory to optional. This is required for the Campus Aggregation switches.

7. Type A-A1 - Access Switches

1.9 Switching Capacity ≥ 300 Gbps

1.10 Forwarding Performance ≥ 40 Mpps

Please accept

1.9	Switching Capacity	≥ 170 Gbps
1.10	Forwarding Performance	≥ 40 Mpps

Comment Accepted

4.6 Proposed equipment must support VLAN-based, 802.1p-based, and MQCbased VLAN mapping

4.9 Proposed equipment must support local and remote port mirroring:

- **MQC Based**
- **ACL Based**

Please remove MQC requirement as it refers to specific vendor.

We were unable to identify any technical standing behind your comment. MQC is a generic term commonly used by many vendors and it stands for "Modular Quality of Service (QoS) Command-Line Interface"

4.19 Proposed equipment must support REP (Resilient Ethernet Protocol), SEP (Smart Ethernet Protection), G.8032 or any equivalent ring protocol which can support less than 50ms failover time

Please remove this specification because this features concerns ring topologies, which are irrelevant to the project, and add extra costs.

This requirement changed from mandatory to optional for the L2 switches (Qty: 14). It still remains mandatory for the L3 switches. Please refer to the response #5.2 for further details.

This requirement concerns "segment" topologies. It is included to add flexibility in cases like ours, when the number of available F/O cabling is limited.

5.2 Proposed equipment must support dynamic routing protocols for IPv4 and IPv6 including:

- **RIP, RIPng**
- **OSPF, OSPFv3**
- **IS-IS**

Please remove this specification because this feature is not necessary in access layer only leading to additional costs

The requirement modified as follows:

The SoC table concerning the Type A-A1 – Access Switches has a typo on the number of required switches. It has to be 24 instead of 23.

The 10 out of the 24 Access Switches need to have L3 capability built-in at the time of purchase.

This is required due to the collapsed Aggregation/Access design in the small scale sites where, there are subsystems requiring local termination on some service VLANs.

The required L3 capabilities are:

"The proposed equipment must support dynamic routing protocols for IPv4 and IPv6 including:

- **RIP, RIPng**

- **OSPF, OSPFv3"**

The required HA requirements on the L3 switches are:

- **1+1 power supply redundancy**
- **Field replaceable Fan Units**

The remaining 14 Access switches can be quoted as L2 switches with light L3 capabilities following the features as requested in the SoC table for "Type A-A1 - Access Switches" excluding the requirement for "7.3 Proposed equipment must support Field replaceable, Hot Swappable FAN module."

9.8 Proposed equipment must support OAM discovery, errored symbol period events, errored frame events, errored frame seconds summary events, fault advertisement, and remote loopback as per IEEE 802.3ah-2004 EFM

Please remove this specification because it is irrelevant to the core switches (refers to last mile Service Provider networks).

We were unable to identify any technical standing behind your comment. This requirement is an industry standard way of monitoring end to end Ethernet network performance. This is required for the Type A-A1 Campus Access switches.

9.7 Proposed equipment must support Alarm Indication Signal (AIS) and delay measurement (DM) as per ITU-T Y.1731

Please remove this specification because it is irrelevant to the core switches, (refers to Service Provider networks).

The requirement changed from mandatory to optional. This is required for the Type A-A1 Campus Access switches.

8. Type B - Access Switches

1.9 Switching Capacity ≥ 300 Gbps

1.10 Forwarding Performance ≥ 40 Mpps

Please accept

1.9	Switching Capacity	≥ 170 Gbps
1.10	Forwarding Performance	≥ 40 Mpps

Comment Accepted

4.6 Proposed equipment must support VLAN-based, 802.1p-based, and MQC based VLAN mapping

4.9 Proposed equipment must support local and remote port mirroring:

- **MQC Based**
- **ACL Based**

Please remove MQC requirement as it refers to specific vendor.

We were unable to identify any technical standing behind your comment. MQC is a generic term commonly used by many vendors and it stands for "Modular Quality of Service (QoS) Command-Line Interface"

4.19 Proposed equipment must support REP (Resilient Ethernet Protocol), SEP (Smart Ethernet Protection), G.8032 or any equivalent ring protocol which can support less than 50ms failover time

Please remove this specification because this feature concerns ring topologies, which are irrelevant to the project, and add extra costs.

This requirement changed from mandatory to optional. This requirement concerns "segment" topologies. It is included to add flexibility in cases like ours, when the number of available F/O cabling is limited.

5.2 Proposed equipment must support dynamic routing protocols for IPv4 and IPv6 including:

- **RIP, RIPng**
- **OSPF, OSPFv3**
- **IS-IS**

Please remove this specification because this feature is not necessary in access layer only leading to additional costs

The requirement on L3 capabilities changed from mandatory to optional. The specific requirement regarding the IS-IS, is removed. The Type B switches can be quoted as L2 switches with light L3 capabilities following the features as requested in the SoC table for "Type B - Access Switches" excluding the requirement for "7.3 Proposed equipment must support Field replaceable, Hot Swappable FAN module." In accordance to the modified requirements on the Type A-A1 L2 switches (Qty 14) with light L3 capabilities.

9.8 Proposed equipment must support OAM discovery, errored symbol period events, errored frame events, errored frame seconds summary events, fault advertisement, and remote loopback as per IEEE 802.3ah-2004 EFM

Please remove this specification because it is irrelevant to the core switches, (refers to last mile Service Provider networks).

We were unable to identify any technical standing behind your comment. This requirement is an industry standard way of monitoring end to end Ethernet network performance. This is required for the Type B Campus Access switches.

9.7 Proposed equipment must support Alarm Indication Signal (AIS) and delay measurement (DM) as per ITU-T Y.1731

Please remove this specification because it is irrelevant to the core switches, (refers to Service Provider networks).

The requirement changed from mandatory to optional. This is required for the Type B Campus Access switches.

9. Type C - Access Switches

1.9 Switching Capacity ≥ 300 Gbps

1.10 Forwarding Performance ≥ 24 Mpps

Please accept

1.9 Switching Capacity ≥ 80 Gbps

1.10 Forwarding Performance ≥ 20 Mpps

Comment Accepted

4.6 Proposed equipment must support VLAN-based, 802.1p-based, and MQCbased VLAN mapping

4.9 Proposed equipment must support local and remote port mirroring:

- **MQC Based**
- **ACL Based**

Please remove MQC requirement as it refers to specific vendor.

We were unable to identify any technical standing behind your comment. MQC is a generic term commonly used by many vendors and it stands for "Modular Quality of Service (QoS) Command-Line Interface"

4.19 Proposed equipment must support REP (Resilient Ethernet Protocol), SEP (Smart Ethernet Protection), G.8032 or any equivalent ring protocol which can support less than 50ms failover time

Please remove this specification because this features concerns ring topologies, which are irrelevant to the project, and add extra costs.

This requirement changed from mandatory to optional. This requirement concerns "segment" topologies. It is included to add flexibility in cases like ours, when the number of available F/O cabling is limited.

5.2 Proposed equipment must support dynamic routing protocols for IPv4 and IPv6 including:

- **RIP, RIPng**
- **OSPF, OSPFv3**
- **IS-IS**

Please remove this specification because this feature is not necessary in access layer only leading to additional costs

The requirement changed from mandatory to optional. The specific requirement regarding the IS-IS, is removed. The Type C switches can be quoted as L2 switches following the features as requested in the SoC table for "Type C - Access Switches".

9.8 Proposed equipment must support OAM discovery, errored symbol period events, errored frame events, errored frame seconds summary events, fault advertisement, and remote loopback as per IEEE 802.3ah-2004 EFM

Please remove this specification because it is irrelevant to the core switches, (refers to last mile Service Provider networks).

We were unable to identify any technical standing behind your comment. This requirement is an industry standard way of monitoring end to end Ethernet network performance. This is required for the Type C Campus Access switches.

9.7 Proposed equipment must support Alarm Indication Signal (AIS) and delay measurement (DM) as per ITU-T Y.1731

Please remove this specification because it is irrelevant to the core switches, (refers to Service Provider networks).

The requirement changed from mandatory to optional. This is required for the Type C Campus Access switches.

10. Internet Routers

2.4 Proposed equipment must support on board, dual personality Electrical and optical Gigabit Ethernet interfaces (IEEE Std 802.3ab, IEEE 802.3z) ≥2

(Per internet router requirement)

Please remove this requirement and accept offers with optical only interfaces, in order to conclude as many vendors as possible being able to contribute to the solution.

This requirement is mandatory due to the fact that Service Provider's CE devices come with Electrical Ethernet Service Interfaces (Customer Router Facing Interfaces) hence the need for Electrical Ethernet Interfaces. You are allowed to offer Electrical SFP interfaces.

3.6 Personal situation criteria

h) ECONOMIC AND FINANCIAL STANDING: A Candidate shall be disqualified if their annual turnover (updated average of last three audited financial years), in not equal to or more than 10.000.000 Euros.

Please clarify that the above disqualification criterion refers to the cumulative turnover of the last three audited financial years.

It is clarified that a candidate shall be disqualified if the cumulative turnover of the last three audited financial years is not equal to or more than 10.000.000 Euros.

5.2 "Submission of offers"

Offers shall be submitted to PPA's Central Protocol, as prescribed in para. 3.3 hereof both in English and in Greek language.

- Does this apply as well for the governmental documents (governemt gazzetes, chamber of commerce certificates etc)?
- Is it expected to translate the SoC in Greek since the tender's language is in English?
- As far as the Datasheets & Product descriptions is concerned it is common practice from the contracting authorities to request it in English or Greek since the vast majority of the offers are from foreign companies who use English as a reference point language not to mention the huge ammount of material need to be translated that renders the whole process extremely time consuming.

Comment Accepted.

3.2 Proposed equipment must support External Clock Synchronization

Please clarify the external clcok synchronization scenario.

This is required for external clock synchronization. The external clock sources are purpose built devices having high clock accuracy. Stratum 1 clocking systems are devices that are directly connected to Stratum 0 highly reliable clock sources such as GPS. In conclusion, the scenario is to be able to have clock synchroznization from external clock sources.

11 Proposed system or systems must support Layer 2 link discovery through LLDP,

CDP, and MAC forwarding table, and Layer 3 IP link discovery by IP addresses.

What is CDP mean here?

CDP stands for Cisco Discovery Protocol. The standards based version of this function is LLDP (Link Layer Discovery protocol). Both protocols are commonly used in our network hence we need support for both of them in the Management System.

1 System architecture.

How many clients will use the management system?

The management system must support the total number of devices requested in the present RFP.

Type A and Type B Switch.

Do these 2 types of access switches need AC power supply?

Proposed equipment must be equipped with power supplies supporting Alternating Current.

Type A 3.1 Optical 10 Gigabit Ethernet (IEEE 802.3ae, 0.3 km over MMF) SFP+ Transceivers.

Why this scenario need so many 10GE SFP+ transceiver modules?

This is the total number of required SFP+ transceivers.

DC switches Electrical Gigabit Ethernet (IEEE 802.3ab) SFP Transceivers.

Does it means that SFP transceiver provide RJ45 interface? Maybe, The "electrical" may be "Optical".?

Proposed equipment must support Electrical 1GbE or Optical (Single mode or Multi Mode fiber) SFP+ transceivers.

DC switches Electrical 100 Gigabit Ethernet (IEEE 802.3ba, High Speed Cable, 5m) QSFP28 Transceivers.

The "electrical" may be "Optical"

We would like to have support for Electrical Direct Attach Cables and Optical Transceivers.

DC switches Proposed equipment must support IEEE 802.1d per VLAN so that multiple instances of the Spanning Tree algorithm can coexist on a physical connection.

802.1D is about STP. STP is a single spanning tree.

802.1d per VLAN may be not defined.

We were unable to understand your question.

DC switches Proposed equipment must support VLAN based STP,RSTP,MSTP.

STP/RSTP is a single spanning tree.
VLAN based STP/RSTP may be not defined.

We were unable to understand your question.

DC Switches: Security.

Could you please tell us detail of this specification?

It is a paragraph header. Below this header, there are requirement that are related to security features.

K6-K8 campus core: Proposed equipment must support IEEE 802.1d per VLAN so that multiple instances of the Spanning Tree algorithm can coexist on a physical connection.

802.1D is about STP. STP is a single spanning tree.
802.1d per VLAN may be not defined.?

We were unable to understand your question.

K6-K8 campus core: Proposed equipment must support VLAN based STP,RSTP,MSTP.

STP/RSTP is a single spanning tree.
VLAN based STP/RSTP may be not defined.

We were unable to understand your question.

K6-K8 campus core: Security.

Could you please tell us detail of this specification?.

It is a paragraph header. Below this header, there are requirement that are related to security features.

K6-K8 campus core: Security.

Could you please tell us detail of this specification?.

It is a paragraph header. Below this header, there are requirement that are related to security features.

DMZ swithes: Electrical Gigabit Ethernet (IEEE 802.3ab) SFP Transceivers.

Does it means that SFP transceiver provide RJ45 interface?Maybe, The "electrical" may be "Optical".?

The service ports on the DMZ switches must be SFP+ based.

DMZ switches: Proposed equipment must support IEEE 802.1d per VLAN so that multiple instances of the Spanning Tree algorithm can coexist on a physical connection.

802.1D is about STP. STP is a single spanning tree.

802.1d per VLAN may be not defined.

We were unable to understand your question.

DMZ switches: Proposed equipment must support VLAN based STP,RSTP,MSTP.

STP/RSTP is a single spanning tree.
VLAN based STP/RSTP may be not defined.

We were unable to understand your question.

DMZ Switches: Security.

Could you please tell us detail of this specification?

It is a paragraph header. Below this header, there are requirement that are related to security features.

K2HQ - Campus Aggregation: Electrical Gigabit Ethernet (IEEE 802.3ab) SFP Transceivers.

Does it means that SFP transceiver provide RJ45 interface?Maybe, The "electrical" may be "Optical".?

The service ports on the Aggregation switches must be SFP+ based.

K2HQ - Campus Aggregation: Proposed equipment must support IEEE 802.1d per VLAN so that multiple instances of the Spanning Tree algorithm can coexist on a physical connection.

802.1D is about STP. STP is a single spanning tree.

802.1d per VLAN may be not defined.

We were unable to understand your question.

K2HQ - Campus Aggregation: Proposed equipment must support VLAN based STP,RSTP,MSTP.

STP/RSTP is a single spanning tree.

VLAN based STP/RSTP may be not defined.

We were unable to understand your question.

K2HQ - Campus Aggregation: Security.

Could you please tell us detail of this specification?

It is a paragraph header. Below this header, there are requirement that are related to security features.

K8 - Campus Aggregation: Electrical Gigabit Ethernet (IEEE 802.3ab) SFP Transceivers.

Does it means that SFP transceiver provide RJ45 interface?Maybe, The "electrical" may be "Optical".?

The service ports on the Aggregation switches must be SFP+ based.

K8 - Campus Aggregation: Proposed equipment must support IEEE 802.1d per VLAN so that multiple instances of the Spanning Tree algorithm can coexist on a physical connection.

802.1D is about STP. STP is a single spanning tree.

802.1d per VLAN may be not defined.

We were unable to understand your question.

K8 - Campus Aggregation: Proposed equipment must support VLAN based STP,RSTP,MSTP.

STP/RSTP is a single spanning tree.

VLAN based STP/RSTP may be not defined.

We were unable to understand your question.

K8 - Campus Aggregation: Security.

Could you please tell us detail of this specification?

It is a paragraph header. Below this header, there are requirement that are related to security features.

K21 - Campus Aggregation: Electrical Gigabit Ethernet (IEEE 802.3ab) SFP Transceivers.

Does it means that SFP transceiver provide RJ45 interface?Maybe, The "electrical" may be "Optical".?

The service ports on the Aggregation switches must be SFP+ based.

K21 - Campus Aggregation: Proposed equipment must support IEEE 802.1d per VLAN so that multiple instances of the Spanning Tree algorithm can coexist on a physical connection.

802.1D is about STP. STP is a single spanning tree.

802.1d per VLAN may be not defined.

We were unable to understand your question.

K21 - Campus Aggregation: Proposed equipment must support VLAN based STP,RSTP,MSTP.

STP/RSTP is a single spanning tree.

VLAN based STP/RSTP may be not defined.

We were unable to understand your question.

K21 - Campus Aggregation: Security.

Could you please tell us detail of this specification?

It is a paragraph header. Below this header, there are requirement that are related to security features.

Type A – A1 – Access Switches: Security.

Could you please tell us detail of this specification?

It is a paragraph header. Below this header, there are requirement that are related to security features.

Type B – Access Switches: Security.

Could you please tell us detail of this specification?

It is a paragraph header. Below this header, there are requirement that are related to security features.

Type C – Access Switches: Security.

Could you please tell us detail of this specification?

It is a paragraph header. Below this header, there are requirement that are related to security features.

B.1 APPENDIX : FINANCIAL OFFER TABLES

For each part of the prices, what are the corresponding trade term? Prices shall be offered based on required trade term.

Please refer to paragraph 7.2 "Payment Terms" of Tender's documentation.

SoC

Please define"Response"standard. May we use "Fully Compliant", "Partially Compliant" and "Non Compliant"?
- "Fully Compliant": meet the requirements of each item
- "Partially Compliant" meet the requirements of each item but not all, or supported by future release, or alternate solution.
- "Non Compliant" cannot meet the requirements of each item.

Answers to the Statement of Compliance tables are response based. The requirements on mandatory items are marked as "YES". Optional requirements are marked as "Optional". Supplier's obligation is to respond on the requirements and

submit evidence documents (reference documents) that support each and every response to each and every requirement.

APPENDIX C: TECHNICAL REQUIREMENT TABLES

Please define"Response"standard. May we use "Fully Compliant" , "Partially Compliant" and "Non Compliant"?
- "Fully Compliant": meet the requirements of each item
- "Partially Compliant" meet the requirements of each item but not all, or supported by future release, or alternate solution.
- "Non Compliant" cannot meet the requirements of each item.

Answers to the Statement of Compliance tables are response based. The requirements on mandatory items are marked as "YES". Optional requirements are marked as "Optional". Supplier's obligation is to respond on the requirements and submit evidence documents (reference documents) that support each and every response to each and every requirement.

APPENDIX C: TECHNICAL REQUIREMENT TABLES

Which kind of power supply is used by DC switches, K6-K8- Campus Core,DMZ Switches,K2HQ - Campus Aggregation,K8 - Campus Aggregation,K21 - Campus Aggregation),Type A-A1 - Access Switches and Type B - Access Switches? It is clear that Campus & DC Firewalls, Type C - Access Switches, External Firewalls and Internet Routers require AC power.

Proposed equipment must be equipped with power supplies supporting Alternating Current

APPENDIX C: TECHNICAL REQUIREMENT TABLES, DC switches

Page 52, item 3.1 Electrical Gigabit Ethernet (IEEE 802.3ab) SFP Transceivers

Does it means that SFP transceiver provide RJ45 interface? Maybe, The "electrical" may be "Optical".

Proposed equipment must support Electrical and Optical (Single mode or Multi Mode fiber) SFP transceivers

APPENDIX C: TECHNICAL REQUIREMENT TABLES, DC switches

Page 52, item 3.3 Optical 40 Gigabit Ethernet (IEEE 802.3ba, 0.1 km over SMF, BIDI) QSFP+ Transceivers

Does BIDI mean single fiber which works duplex mode?

BIDI transceiver means a transceiver that supports bidirectional transmission over a single F/O cable by using different wavelengths

APPENDIX C: TECHNICAL REQUIREMENT TABLES, DC switches

Page 53, item 4.18 Proposed equipment must support IEEE 802.1d per VLAN so that multiple instances of the Spanning Tree algorithm can coexist on a physical connection.

802.1D is about STP. STP is a single spanning tree. 802.1d per VLAN may be not defined.

We were unable to understand your question

APPENDIX C: TECHNICAL REQUIREMENT TABLES, DC switches

Page 53, item 4.22 Proposed equipment must support VLAN based STP, RSTP, MSTP.

STP/RSTP is a single spanning tree. VLAN based STP/RSTP may be not defined.

We were unable to understand your question

APPENDIX C: TECHNICAL REQUIREMENT TABLES, DC switches

Page 57, item 11.1 Security

Could you please tell us detail of this specification?

It is a paragraph header. Below this header, there are requirement that are related to security features

APPENDIX C: TECHNICAL REQUIREMENT TABLES, K6-K8 Campus Core

Page 58, item 1.2 2

The total quantity of core switch in K6 and K8 is 2? In page 7， the quantity of campus core switch is 4.

The current design is based on 4 campus core switches that are located in buildings K6 and K8. Each Campus Core node, has one pair of Campus Core Switches serving a specific "island" of Aggregation Nodes. The new design will have two Campus Core Switches in total, interconnected with optical Back to Back interconnections forming a cluster. This is based on the assumption that each and every Aggregation node will be interconnected to both Core Nodes that are located in buildings K6 and K8.

APPENDIX C: TECHNICAL REQUIREMENT TABLES, K6-K8 Campus Core

Page 59, item 3.1 Number of 1 Gigabit Ethernet SFP transceivers (0.1 km over CAT6 copper cabling)

Does it means that SFP transceiver provide RJ45 interface?

The service ports on the line cards of the Campus Core switches must be SFP or SFP+ based in order to support Electrical 1GbE

APPENDIX C: TECHNICAL REQUIREMENT TABLES, K6-K8 Campus Core

Page 60, item 4.11 Proposed equipment must support IEEE 802.1d per VLAN so that multiple instances of the Spanning Tree algorithm can coexist on a physical connection

802.1D is about STP. STP is a single spanning tree. 802.1d per VLAN may be not defined.

We were unable to understand your question

APPENDIX C: TECHNICAL REQUIREMENT TABLES, K6-K8 Campus Core

Page 60, item 4.14 Proposed equipment must support VLAN based STP, RSTP, MSTP

STP/RSTP is a single spanning tree. VLAN based STP/RSTP may be not defined.

We were unable to understand your question

APPENDIX C: TECHNICAL REQUIREMENT TABLES, K6-K8 Campus Core

Page 64, item 11.1 Security

Could you please tell us detail of this specification?

It is a paragraph header. Below this header, there are requirements that are related to security features

APPENDIX C: TECHNICAL REQUIREMENT TABLES, DMZ Switches

Page 69, item 3.1 Electrical Gigabit Ethernet (IEEE 802.3ab) SFP Transceivers

Does it means that SFP transceiver provide RJ45 interface? Maybe, The "electrical" may be "Optical".

The service ports on the switches must be SFP+ based supporting Electrical GbE transceivers

APPENDIX C: TECHNICAL REQUIREMENT TABLES, DMZ Switches

Page 70, item 4.12 Proposed equipment must support IEEE 802.1d per VLAN so that multiple instances of the Spanning Tree algorithm can coexist on a physical connection.

802.1D is about STP. STP is a single spanning tree. 802.1d per VLAN may be not defined.

We were unable to understand your question

APPENDIX C: TECHNICAL REQUIREMENT TABLES, DMZ Switches

Page 70, item 4.16 Proposed equipment must support VLAN based STP, RSTP, MSTP

STP/RSTP is a single spanning tree. VLAN based STP/RSTP may be not defined.

We were unable to understand your question

APPENDIX C: TECHNICAL REQUIREMENT TABLES, DMZ Switches

Page 74, item 11.1 Security

Could you please tell us detail of this specification?

It is a paragraph header. Below this header, there are requirements that are related to security features

APPENDIX C: TECHNICAL REQUIREMENT TABLES, K2HQ - Campus Aggregation

Page 76, item 3.1 Electrical Gigabit Ethernet (IEEE 802.3ab) SFP Transceivers

Does it means that SFP transceiver provide RJ45 interface? Maybe, The "electrical" may be "Optical".

The service ports on the switches must be SFP+ based supporting Electrical GbE transceivers

APPENDIX C: TECHNICAL REQUIREMENT TABLES, K2HQ - Campus Aggregation

Page 77, item 4.12 Proposed equipment must support IEEE 802.1d per VLAN so that multiple instances of the Spanning Tree algorithm can coexist on a physical connection.

802.1D is about STP. STP is a single spanning tree. 802.1d per VLAN may be not defined.

We were unable to understand your question

APPENDIX C: TECHNICAL REQUIREMENT TABLES, K2HQ - Campus Aggregation

Page 77, item 4.16 Proposed equipment must support VLAN based STP, RSTP, MSTP

STP/RSTP is a single spanning tree. VLAN based STP/RSTP may be not defined.

We were unable to understand your question

APPENDIX C: TECHNICAL REQUIREMENT TABLES, K2HQ - Campus Aggregation

Page 81, item 11.1 Security

Could you please tell us detail of this specification?

It is a paragraph header. Below this header, there are requirements that are related to security features

APPENDIX C: TECHNICAL REQUIREMENT TABLES, K8 - Campus Aggregation

Page83, item 3.1 Electrical Gigabit Ethernet (IEEE 802.3ab) SFP Transceivers

Does it means that SFP transceiver provide RJ45 interface? Maybe, The "electrical" may be "Optical".

The service ports on the switches must be SFP+ based supporting Electrical GbE transceivers

APPENDIX C: TECHNICAL REQUIREMENT TABLES, K8 - Campus Aggregation

Page 84, item 4.12 Proposed equipment must support IEEE 802.1d per VLAN so that multiple instances of the Spanning Tree algorithm can coexist on a physical connection.

802.1D is about STP. STP is a single spanning tree. 802.1d per VLAN may be not defined.

We were unable to understand your question

APPENDIX C: TECHNICAL REQUIREMENT TABLES, K8 - Campus Aggregation

Page 84, item 4.16 Proposed equipment must support VLAN based STP, RSTP, MSTP

STP/RSTP is a single spanning tree. VLAN based STP/RSTP may be not defined.

We were unable to understand your question

APPENDIX C: TECHNICAL REQUIREMENT TABLES, K8 - Campus Aggregation

Page 88, item 11.1 Security

Could you please tell us detail of this specification?

It is a paragraph header. Below this header, there are requirements that are related to security features

APPENDIX C: TECHNICAL REQUIREMENT TABLES, K21 - Campus Aggregation

Page 90, item 3.1 Electrical Gigabit Ethernet (IEEE 802.3ab) SFP Transceivers

Does it means that SFP transceiver provide RJ45 interface? Maybe, The "electrical" may be "Optical".

The service ports on the switches must be SFP+ based supporting Electrical GbE transceivers

APPENDIX C: TECHNICAL REQUIREMENT TABLES, K21 - Campus Aggregation

Page 91, item 4.12 Proposed equipment must support IEEE 802.1d per VLAN so that multiple instances of the Spanning Tree algorithm can coexist on a physical connection.

802.1D is about STP. STP is a single spanning tree. 802.1d per VLAN may be not defined.

We were unable to understand your question

APPENDIX C: TECHNICAL REQUIREMENT TABLES, K21 - Campus Aggregation

Page 92, item 4.16 Proposed equipment must support VLAN based STP, RSTP, MSTP

STP/RSTP is a single spanning tree. VLAN based STP/RSTP may be not defined.

We were unable to understand your question

APPENDIX C: TECHNICAL REQUIREMENT TABLES, K21 - Campus Aggregation

Page 95, item 11.1 Security

Could you please tell us detail of this specification?

It is a paragraph header. Below this header, there are requirements that are related to security features

APPENDIX C: TECHNICAL REQUIREMENT TABLES, Type A-A1 - Access Switches

Page 102, item 11.1 Security

Could you please tell us detail of this specification?

It is a paragraph header. Below this header, there are requirements that are

related to security features

APPENDIX C: TECHNICAL REQUIREMENT TABLES, Type B - Access Switches

Page 109, item 11.1 Security

Could you please tell us detail of this specification?

It is a paragraph header. Below this header, there are requirements that are related to security features

APPENDIX C: TECHNICAL REQUIREMENT TABLES, Type C - Access Switches

Page 115, item 11.1 Security

Could you please tell us detail of this specification?

It is a paragraph header. Below this header, there are requirements that are related to security features

APPENDIX C: TECHNICAL REQUIREMENT TABLES, Cabling Works

Questions:

1. Are there layouts for the Project?
2. Are construction work included in the project?
3. Can we make an on-site visit to PPA and when?

1. **The project involves the replacement of network equipment. Changes in the infrastructure will not be done except for the upgrading of the cabling in the central building of the OLP (Regarding the K2 (Headquarters) center building at the points where the local rack connection with the corresponding distribution switch is made with a copper Wire, the contractor should take over to implement the fiber optic interface. The connection cable should be OM4 - Laser-Optimized Multimode. Those interested can visit the PPA premises for more detailed recording.) We would like you to clarify what plans-diagrams you are referring to and why you need them.**
2. **The answer has been given to the previous question**
3. **If you are interested, we can immediately arrange an on-site visit to our facilities**