



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

**EQUIPOS ACTIVOS DE RED
EDIFICIO LABORATORIOS DE INGENIERÍA**



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

CONTENIDO

1. DESCRIPCIÓN DEL CONTEXTO TÉCNICO	3
2. OBJETO DEL PROCESO	3
3. ALCANCE DEL OBJETO.....	4
4. CONDICIONES GENERALES.....	4
5. REQUERIMIENTOS TÉCNICOS NETWORKING LAN.....	6
6. REQUERIMIENTOS TÉCNICOS NETWORKING WLAN.....	22
7. REQUERIMIENTOS DE DESEMPEÑO.....	24
8. PRUEBAS Y CRITERIOS DE ACEPTACIÓN	25
9. GARANTÍA Y SOPORTE.....	26



UNIVERSIDAD DISTRICTAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

1. DESCRIPCIÓN DEL CONTEXTO TÉCNICO

La Universidad Distrital Francisco José de Caldas cuenta con una arquitectura de red en topología estrella, en la que convergen 15 sedes del campus universitario a través de una WAN conformada por 15 enlaces dedicados de datos, aprovisionados por el ISP actual. Estos enlaces garantizan la conectividad de toda la comunidad universitaria y permiten el acceso a los diferentes servicios desplegados en la red convergente.

La infraestructura de Networking LAN principalmente está compuesta por equipos de conmutación de la marca Cisco® y algunos equipos de la marca Juniper®, instalados y en operación en las distintas sedes. En el caso de Cisco®, se dispone de switches de las series 9500, 9300, entre otros; mientras que, para Juniper®, se cuenta con equipos de las series EX4300, EX4600 y QFX5100. En el nodo central de la Universidad ubicado en la sede calle 40, se cuenta con equipos switch core Cisco® C9500 en configuración StackWise para el núcleo, y equipos C9300 en stack para la capa de acceso. Esta infraestructura permite la interconexión entre sedes y soporta los servicios alojados en el datacenter Olimpo.

En cuanto a la infraestructura WLAN, la Universidad tiene desplegada una solución Cisco® que incluye controladoras de las series C9800, así como Access Point (puntos de acceso) de las series C9120AXI y C9124AXI.

Adicionalmente, se dispone de plataformas de control de acceso a la red (NAC), específicamente Cisco® ISE (Identity Services Engine), así como de la plataforma Cisco® DNA (Digital Network Architecture) para la gestión y automatización de la red.

Actualmente se encuentra en construcción el edificio de laboratorios de la Facultad de Ingeniería, el cual debe ser integrado a la infraestructura de red de la sede Calle 40.

2. OBJETO DEL PROCESO

Suministrar, instalar, configurar e implementar una solución de Networking LAN y WLAN, que incluya equipos, hardware, software, licenciamiento y demás componentes de telecomunicaciones, con el fin de garantizar el acceso eficiente y confiable a los servicios de red de la Universidad, de acuerdo con los términos de referencia.



UNIVERSIDAD DISTRICTAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

3. ALCANCE DEL OBJETO

- Implementar una solución de Networking LAN y WLAN que incluya el suministro, instalación, configuración e implementación de equipos de conmutación (switches) y puntos de acceso (Access Point) tipo indoor y outdoor, junto con sus respectivos componentes, accesorios, licenciamiento y soporte. Esta solución deberá integrarse con la red corporativa de la Universidad, permitiendo brindar conectividad a las diferentes áreas de trabajo y dispositivos en las sedes que la Universidad defina, garantizando alto rendimiento en las comunicaciones de red.
- La solución deberá permitir la gestión del acceso a la red mediante la autenticación de usuarios, a través de su integración con la red convergente y con las plataformas Cisco® ISE (NAC) y Cisco® DNA, así como con el directorio activo Microsoft® actualmente implementado en la Universidad.
- Los equipos, componentes y accesorios adquiridos deberán contar con servicio de licenciamiento, soporte, garantía y reemplazo de partes por un periodo de mínimo cinco (5) años, bajo un esquema de atención 8x5xNBD (8 horas diarias, 5 días hábiles a la semana, con reemplazo de hardware al siguiente día hábil), de acuerdo con las condiciones establecidas.
- Los equipos y componentes objeto del presente proceso deberán soportar los protocolos IPv4 e IPv6. El soporte de IPv6 deberá estar certificado mediante el programa IPv6 Ready Logo.
- La solución a implementar estará compuesta por dos (2) componentes:
 - Networking LAN
 - Networking WLAN.

4. CONDICIONES GENERALES

- a. El contratista deberá realizar visitas previas a la sede donde se llevará a cabo la instalación de los equipos, con el fin de efectuar la ingeniería de detalle requerida para su posterior instalación y puesta en funcionamiento.
- b. La totalidad de los equipos, módulos, fuentes y demás componentes ofertados deberán ser de la misma marca que la solución propuesta.



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

- c. Los productos adquiridos deberán ser nuevos, originales, ensamblados en fábrica y registrados a nombre de la Universidad Distrital Francisco José de Caldas. Los equipos deberán entregarse en sus empaques originales, debidamente sellados. La Universidad, a través de la supervisión, verificará en todo momento el cumplimiento de las condiciones de originalidad y estado de los equipos y/o componentes adquiridos en el marco del presente proceso.
- d. Todos los equipos deberán entregarse con la última versión de software disponible y estable al momento de la entrega. Durante la vigencia del servicio de soporte y licenciamiento, deberán actualizarse a las versiones estables que libere el fabricante, previa autorización de la supervisión o quien la supervisión designe.
- e. Para cada equipo se deberán contemplar todos los accesorios, cables de poder, módulos, licenciamiento y demás componentes necesarios para su instalación, puesta en funcionamiento e integración con las plataformas existentes de la Universidad, tales como Cisco® ISE (Identity Services Engine) y Cisco® DNA (Digital Network Architecture).
- f. Los equipos y componentes serán entregados en el sitio que la supervisión determine durante la ejecución del contrato. En caso de requerirse su traslado al sitio final de instalación, el contratista será responsable del transporte, fletes y seguros, sin que ello genere costos adicionales para la Universidad.
- g. Toda la instalación de hardware y software deberá ser realizada por personal certificado por el fabricante. Durante la ejecución del contrato, se deberán suministrar las certificaciones del personal técnico.
- h. Cualquier implementación no deberá afectar la garantía ni el correcto funcionamiento de los equipos y sistemas actualmente instalados, ni de los espacios físicos intervenidos.
- i. El contratista deberá contemplar todos los elementos, dispositivos y mecanismos necesarios para la ejecución de trabajos en alturas, en cumplimiento de la normativa vigente.
- j. El contratista deberá considerar los diferentes tipos de techos presentes en la sede de la Universidad, proyectando los elementos adicionales requeridos para la instalación de los equipos (chazos, amarres, soportes, mástiles, entre otros). Toda la solución deberá implementarse bajo la modalidad llave en mano.
- k. Realizar una transferencia de conocimiento con una duración de doce (12) horas, dirigida al personal técnico designado por la Supervisión, que incluya temas de troubleshooting, administración y gestión de los equipos de la solución LAN–WLAN.
- l. La implementación, mantenimiento y/o soporte por parte del contratista no deberá afectar el funcionamiento ni la garantía de los equipos y subsistemas existentes en el Datacenter ni de los espacios físicos. A partir del momento en que se otorgue acceso a los centros de gestión, cuartos de telecomunicaciones y equipos de la Universidad, el contratista asumirá total responsabilidad por la integridad física de



UNIVERSIDAD DISTRICTAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

- los elementos intervenidos y su entorno, comprometiéndose a realizar un manejo adecuado que evite su deterioro, degradación o daño físico.
- m. Por cada actividad de soporte y/o mantenimiento realizado, el contratista deberá entregar un informe técnico escrito en un plazo no mayor a cinco (5) días hábiles, de conformidad con lo establecido en el numeral 9. Garantía y soporte” del presente documento.
 - n. El oferente, en su propuesta, debe entregar las fichas técnicas de todos los equipos propuestos.

5. REQUERIMIENTOS TÉCNICOS NETWORKING LAN

5.1. Equipos Core – Data Center Olimpo

Se requiere ampliar la solución Core-Datacenter actual del datacenter Olimpo (Sede Calle 40) para recibir las conexiones del edificio de laboratorios de la siguiente manera:

- a. Suministrar, instalar y configurar una solución Core–Datacenter en el Data Center Olimpo, conformada por dos (2) equipos switches de acuerdo con la Tabla 1. “*Requerimientos técnicos Switch Core 48P – Datacenter*” en configuración de alta disponibilidad (HA), garantizando la interconexión con los equipos de red ubicados en los cuartos de telecomunicaciones del edificio de laboratorios, así como con los sistemas alojados en el Datacenter y con la infraestructura Core existente.
- b. Los equipos deberán instalarse en configuración de stack (apilamiento), mediante tecnología Stackwise los equipos *Switch Core 48 P– Datacenter* con la solución de Core Cisco Catalyst 9500-48Y4C de la Universidad quedando un único equipo lógico el cual deberá ser administrando y gestionado por una única IP.
- c. Cada equipo debe contar con los cuarenta y ocho (48) módulos transceptor necesarios para fibra óptica, compatible, programado y probado para su funcionamiento con enrutadores y conmutadores, los cuales deben ofrecer conectividad 10GbE fiable a través de cable de fibra óptica MULTIMODO para redes compatibles con 10GBASE-SR, con una distancia máxima de hasta 400m. de acuerdo a las especificaciones de la Tabla 6. “*Requerimientos técnicos módulo transceiver SFP+*”.
- d. Integrar los switches de la solución a proveer con las plataformas Cisco® DNA, Cisco® NAC (ISE) de la Universidad.



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

REQUERIMIENTOS TÉCNICOS SWITCH CORE 48 P – DATACENTER	
Ítem	Descripción
1	Debe tener mínimo 48 puertos Non-Blocking para conector de fibra multimodo a 1/10/25 Gbps con negociación automática (SFP/SFP+/SFP28)
2	Debe tener mínimo 4 puertos 40/100 GE (QSFP+/QSFP28) para uplinks de alta velocidad.
3	Debe soportar configuraciones de apilamiento virtual, unificándose e integrándose con la solución switch core de la Universidad como si fueran el mismo switch lógico.
4	Debe permitir configurar, soportar e incluir las licencias para habilitar o configurar los protocolos: <ul style="list-style-type: none">• OSPFv3• VRRPv3• BGPv4• ARP• IGMPv3• SNMPv3• DHCP Server• DHCP relay• NTP• Enrutamiento estático• Enrutamiento virtual (VRF)• EVPN con VXLAN• SSH v2• ACL (IPv4 e IPv6)
5	DRAM mínima 16 GB.
6	FLASH mínima 16 GB.
7	El equipo debe ser “ <i>non-blocking</i> ”, esto es, que la matriz de conmutación permita simultáneamente el manejo de todos los puertos a su máxima capacidad full dúplex sin bloquearse o sin presentar sobresuscripción, es decir que el equipo soporte mínimo 3.2 Tbps en switching capacity.
8	Los equipos deben poder realizar apilamiento (agrupación o chasis virtual) por medio de cable y módulos propios del fabricante requeridos para su correcto funcionamiento y deberán ser incluidos.
9	Soportar mínimo 32000 direcciones MAC.
10	Soportar mínimo 16000 rutas Multicast IPv4 y mínimo 16000 rutas Multicast IPv6.
11	Soporte de Dual stack para IPv4/IPv6
12	Soporte de IPv6 y enrutamiento IPv6 en hardware, ya que se requiere desempeño sin sobresuscripción para tráfico y servicios IPv6.



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

REQUERIMIENTOS TÉCNICOS SWITCH CORE 48 P – DATACENTER	
Ítem	Descripción
13	Debe soportar las siguientes funcionalidades de enrutamiento para multicast en IPv6: a. Protocol Independent Multicast b. PIM in Source Specific Multicast (PIM-SSM)
14	Soportar mínimo 64000 rutas IPv4 ARP
15	Soportar mínimo 4000 VLAN ID.
16	Debe soportar Jumbo frame mínimo de 9000 bytes.
17	Debe soportar tasa mínima de reenvío de paquetes (Forwarding Rate) de 900 Mpps.
18	Debe cumplir con los siguientes RFC, funcionalidades y estándares: <ul style="list-style-type: none">• RFC2460 (IPv6 Basic specification)• RFC4291 (IPv6 Addressing Architecture)• RFC3484 (Default Address Selection)• RFC4193 (Unique Local IPv6 Unicast Addresses (ULA))• RFC4443 (ICMPv6)• RFC4862 (SLAAC)• RFC3810 (Multicast Listener Discovery Version 2 (MLDv2) for IPv6)• RFC2711 (Router-Alert option)• RFC1981 (Path MTU Discovery)• RFC4861 (Neighbor Discovery)• RFC5095 (Deprecation of Type 0 Routing Headers in IPv6)• RFC3315 (DHCPv6 filtering)• RFC4861 (Dynamic "IPv6 Neighbor solicitation/advertisement" inspection / Neighbor Unreachability Detection filtering)• RFC4862 (IPv6 Stateless Address Autoconfiguration)• OSPFv3: RFC5340, RFC4552 y RFC 5838• IEEE 802.1AB LLDP• IEEE 802.1D Spanning Tree Protocol• IEEE 802.1p CoS prioritization• IEEE 802.1Q VLAN• IEEE 802.1s RSTP• IEEE 802.1w• IEEE 802.1x• IEEE 802.3ad LACP• IEEE 802.3x
19	Soporte de 802.1X, MACsec-256 o MACsec AES 256. Debe soportar funcionalidades de seguridad que permitan detectar amenazas en la red, tales como ataques de comando y control, ransomware, DDoS, malware desconocido, y amenazas internas, incluso si se producen sobre tráfico cifrado.



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

REQUERIMIENTOS TÉCNICOS SWITCH CORE 48 P – DATACENTER	
Ítem	Descripción
20	El equipo debe ser administrado a través de CLI, WEB, SNMP, SSH.
21	Debe tener luces indicadoras de múltiples funciones como estado del equipo y estado de puertos
22	El equipo debe contar con mínimo dos (2) fuentes de poder de mínimo 650 W y deben ser hotswap. Alimentadas en un margen de 110VAC - 220 VAC
23	El MTBF ofrecido por el fabricante debe ser como mínimo de 300000 h
24	Los equipos deben soportar e incluir funciones de programabilidad por medio de scripting en Python y soporte de APIs (Application Programmable Interfaces)
25	Debe estar en capacidad de soportar e incluir los siguientes protocolos de gestión y automatización: NETCONF y/o YANG, ZTP y/o Open PnP y/o equivalente que permita realizar implementación automática de dispositivos de red (Switch) desde un controlador SDN.
26	Los equipos deben estar en capacidad de formar un fabric tipo SDN por medio de la virtualización de la red con mecanismos de EVPN con VXLAN.
27	Los equipos deben soportar las siguientes funcionalidades tipo SDN: <ul style="list-style-type: none">• Implementación automatizada tipo Zero-Touch• Visibilidad de endpoints y usuarios para funciones de troubleshooting: Analíticas y Telemetría.• Políticas de segmentación y microsegmentación basadas en grupos de objetos (IPv4 e IPv6).• Soportar la integración con un controlador tipo SDN que simplifique la administración y orquestación de la solución.
28	El equipo debe poderse montar en racks de 19 pulgadas e incluir los herrajes para su montaje.
29	Debe incluir cable de conexión y accesorios para apilamiento virtual
30	Licenciamiento necesario para la integración a las plataformas Cisco® DNA, Cisco® NAC (ISE).

Tabla 1. Requerimientos técnicos Switch Core 48P – Datacenter

5.2. Equipos Core – Data Center CECAD

- Suministrar la solución Core–Datacenter con destino al Data Center del CECAD, conformada por dos (2) equipos switches de acuerdo con la Tabla 2. “*Requerimientos técnicos Switch Core 24P – Datacenter*” en configuración de alta disponibilidad (HA), garantizando la interconexión con los equipos de red y sistemas alojados en el Data Center del CECAD.



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

- b. Los equipos deberán instalarse en configuración de stack (apilamiento), con el fin de asegurar alta disponibilidad con los equipos de red que actualmente se tienen en la Universidad.
- c. Cada equipo debe contar con los veinticuatro (28) módulos transceptor necesarios para fibra óptica, compatible, programado y probado para su funcionamiento con enrutadores y conmutadores, los cuales deben ofrecer conectividad 10GbE fiable a través de cable de fibra óptica MULTIMODO para redes compatibles con 10GBASE-SR, con una distancia máxima de hasta 400m. de acuerdo a las especificaciones de la Tabla 6. “*Requerimientos técnicos módulo transceiver SFP+*”.
- d. Realizar la integración y configuración necesarias para asegurar la correcta interoperabilidad con la infraestructura actual de Datacenter y de campus.

REQUERIMIENTOS TÉCNICOS SWITCH CORE 24P – DATACENTER	
Ítem	Descripción
1	Debe tener mínimo 24 puertos Non-Blocking para conector de fibra multimodo a 1/10/25 Gbps con negociación automática (SFP/SFP+/SFP28)
2	Debe tener mínimo 4 puertos 40/100 GE (QSFP+/QSFP28) para uplinks de alta velocidad.
3	Debe soportar configuraciones de apilamiento virtual, que permita unificar mínimo dos (2) unidades de switches de Core/distribución como si fueran el mismo switch lógico.
4	Debe permitir configurar, soportar e incluir las licencias para habilitar o configurar los protocolos: <ul style="list-style-type: none">• OSPFv3• VRRPv3• BGPv4• ARP• IGMPv3• SNMPv3• DHCP Server• DHCP relay• NTP• Enrutamiento estático• Enrutamiento virtual (VRF)• EVPN con VXLAN• SSH v2• ACL (IPv4 e IPv6)
5	DRAM mínima 16 GB.



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

REQUERIMIENTOS TÉCNICOS SWITCH CORE 24P – DATACENTER	
Ítem	Descripción
6	FLASH mínima 16 GB.
7	El equipo debe ser “ <i>non-blocking</i> ”, esto es, que la matriz de conmutación permita simultáneamente el manejo de todos los puertos a su máxima capacidad full dúplex sin bloquearse o sin presentar sobresuscripción, es decir que el equipo soporte mínimo 2.0 Tbps en switching capacity.
8	Los equipos deben poder realizar apilamiento (agrupación o chasis virtual) por medio de cable y módulos propios del fabricante requeridos para su correcto funcionamiento y deberán ser incluidos.
9	Soportar mínimo 32000 direcciones MAC.
10	Soportar mínimo 16000 rutas Multicast IPv4 y mínimo 16000 rutas Multicast IPv6.
11	Soporte de Dual stack para IPv4/IPv6
12	Soporte de IPv6 y enrutamiento IPv6 en hardware, ya que se requiere desempeño sin sobresuscripción para tráfico y servicios IPv6.
13	Debe soportar las siguientes funcionalidades de enrutamiento para multicast en IPv6: <ul style="list-style-type: none">• Protocol Independent Multicast• PIM in Source Specific Multicast (PIM-SSM)
14	Soportar mínimo 64000 rutas IPv4 ARP
15	Soportar mínimo 4000 VLAN ID.
16	Debe soportar Jumbo frame mínimo de 9000 bytes.
17	Debe soportar tasa mínima de reenvío de paquetes (Forwarding Rate) de 900 Mpps.
18	Debe cumplir con los siguientes RFC, funcionalidades y estándares: <ul style="list-style-type: none">• RFC2460 (IPv6 Basic specification)• RFC4291 (IPv6 Addressing Architecture)• RFC3484 (Default Address Selection)• RFC4193 (Unique Local IPv6 Unicast Addresses (ULA))• RFC4443 (ICMPv6)• RFC4862 (SLAAC)• RFC3810 (Multicast Listener Discovery Version 2 (MLDv2) for IPv6)• RFC2711 (Router-Alert option)• RFC1981 (Path MTU Discovery)• RFC4861 (Neighbor Discovery)• RFC5095 (Deprecation of Type 0 Routing Headers in IPv6)• RFC3315 (DHCPv6 filtering)• RFC4861 (Dynamic "IPv6 Neighbor solicitation/advertisement" inspection / Neighbor Unreachability Detection filtering)• RFC4862 (IPv6 Stateless Address Autoconfiguration)



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

REQUERIMIENTOS TÉCNICOS SWITCH CORE 24P – DATACENTER	
Ítem	Descripción
	<ul style="list-style-type: none">• OSPFv3: RFC5340, RFC4552 y RFC 5838• IEEE 802.1AB LLDP• IEEE 802.1D Spanning Tree Protocol• IEEE 802.1p CoS prioritization• IEEE 802.1Q VLAN• IEEE 802.1s RSTP• IEEE 802.1w• IEEE 802.1x• IEEE 802.3ad LACP• IEEE 802.3x
19	Soporte de 802.1X, MACsec-256 o MACsec AES 256. Debe soportar funcionalidades de seguridad que permitan detectar amenazas en la red, tales como ataques de comando y control, ransomware, DDoS, malware desconocido, y amenazas internas, incluso si se producen sobre tráfico cifrado.
20	El equipo debe ser administrado a través de CLI, WEB, SNMP, SSH.
21	Debe tener luces indicadoras de múltiples funciones como estado del equipo y estado de puertos
22	El equipo debe contar con mínimo dos (2) fuentes de poder de mínimo 650 W y deben ser hotswap. Alimentadas en un margen de 110VAC - 220 VAC
23	El MTBF ofrecido por el fabricante debe ser como mínimo de 300000 h
24	Los equipos deben soportar e incluir funciones de programabilidad por medio de scripting en Python y soporte de APIs (Application Programmable Interfaces)
25	Debe estar en capacidad de soportar e incluir los siguientes protocolos de gestión y automatización: NETCONF y/o YANG, ZTP y/o Open PnP y/o equivalente que permita realizar implementación automática de dispositivos de red (Switch) desde un controlador SDN.
26	Los equipos deben estar en capacidad de formar un fabric tipo SDN por medio de la virtualización de la red con mecanismos de EVPN con VXLAN.
27	Los equipos deben soportar las siguientes funcionalidades tipo SDN: <ul style="list-style-type: none">• Implementación automatizada tipo Zero-Touch• Visibilidad de endpoints y usuarios para funciones de troubleshooting: Analíticas y Telemetría.• Políticas de segmentación y microsegmentación basadas en grupos de objetos (IPv4 e IPv6).• Soportar la integración con un controlador tipo SDN que simplifique la administración y orquestación de la solución.
28	Debe incluir cable de conexión y accesorios para apilamiento virtual



Tabla 2. Requerimientos técnicos Switch Core 24P – Datacenter

5.3. Equipos Conmutación

- Suministrar los switches de acceso, incluyendo su respectivo licenciamiento, soporte, garantía, módulos, fuentes de poder y accesorios, en cumplimiento de las condiciones técnicas exigidas.
- Los equipos deberán instalarse en configuración de stack (apilamiento), con el fin de asegurar un alto rendimiento, fiabilidad, redundancia y facilidad de gestión (cuando sea necesario).
- Cada stack físico ubicado en cada cuarto de telecomunicaciones deberá contar con mínimo cuatro (4) módulos transceptor necesarios para fibra óptica, compatible, programado y probado para su funcionamiento con enrutadores y conmutadores, los cuales deben ofrecer conectividad 10GbE fiable a través de cable de fibra óptica MULTIMODO para redes compatibles con 10GBASE-SR, con una distancia máxima de hasta 400m. de acuerdo a las especificaciones de la Tabla 6. “*Requerimientos técnicos módulo transceiver SFP+*”. Estos módulos serán los responsables de realizar la interconexión con el switch Core ubicado en el Data Center Olimpo.
- Realizar la integración y configuración necesaria para asegurar la correcta interoperabilidad con la infraestructura actual de Datacenter y de campus.
- Todos los switches de acceso deberán integrarse con el appliance Cisco® DNA (Digital Network Architecture) versión 2.3.7.7 y el controlador de acceso a la red Cisco® ISE (Identity Services Engine) a efectos de aprovechar los recursos, tecnologías y plataformas de administración de la Universidad, por lo tanto, el proponente debe suministrar las licencias advantage necesarias para los equipos switches sobre la plataforma DNA e ISE, las cuales deben estar contempladas en la oferta económica.

5.3.1. Switch acceso multigigabit

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 48 PTS MULTIGIGABIT	
Ítem	Descripción
1	Debe tener mínimo 48 puertos Non-Blocking para conector RJ-45 autosensing 10/100/1000 o 100/1000 MDIX con PoE de 1100W de los cuales mínimo 12 deben ser Multigigabit 100/1G/2,5G/5G
2	Debe tener mínimo 4 puertos de uplink a 10G SFP+ para uplinks de alta velocidad
3	Deben soportar configuraciones de apilamiento de mínimo 8 equipos (entre Switches de Acceso de la misma familia) y se debe tener gestión de los mismos por medio de una única dirección ip



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 48 PTS MULTIGIGABIT	
Ítem	Descripción
4	Debe soportar los siguientes protocolos: <ul style="list-style-type: none">• OSPFv3• VRRPv3• BGPv4• ARP• IGMPv3• SNMPv3• DHCP Server• DHCP relay• NTP• Enrutamiento estático• Enrutamiento virtual (VRF)• EVPN con VXLAN• SSH v2• ACL (IPv4 e IPv6)
5	DRAM mínima 8GB
6	FLASH mínimo 16GB
7	El equipo debe ser " <i>non-blocking</i> ", esto es, que la matriz de conmutación permita simultáneamente el manejo de todos los puertos a su máxima capacidad full dúplex sin bloquearse o sin presentar sobresuscripción, es decir que el equipo soporte mínimo 520 Gbps en switching capacity, sin contar el throughput del módulo físico de stack.
8	El switching capacity del stacking debe ser físico de mínimo 1000 Gbps, que permita tener hasta 8 miembros.
9	Soportar mínimo 32.000 direcciones MAC
10	Soportar mínimo 32000 rutas IPv4 ARP plus learned routes – (24,000 directas y 8,000 indirectas)
11	Soportar mínimo 16000 rutas de enrutamiento en IPv6
12	Soporte de Dual stack para IPv4/IPv6
13	Soporte de IPv6 y enrutamiento IPv6 en hardware, ya que se requiere desempeño sin sobresuscripción para tráfico y servicios IPv6.
14	Soportar mínimo 4000 VLAN ID
15	Debe soportar Jumbo frame mínimo de 9100 bytes
16	Debe soportar tasa mínima de reenvío de paquetes (Forwarding Rate) de 400 Mpps.
17	Debe cumplir con los siguientes RFC, funcionalidades y estándares: <ul style="list-style-type: none">• RFC2460 (IPv6 Basic specification)• RFC4291 (IPv6 Addressing Architecture)• RFC3484 (Default Address Selection)• RFC4193 (Unique Local IPv6 Unicast Addresses (ULA))



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 48 PTS MULTIGIGABIT	
Ítem	Descripción
	<ul style="list-style-type: none">• RFC4443 (ICMPv6)• RFC4862 (SLAAC)• RFC1981 (Path MTU Discovery)• RFC4861 (Neighbor Discovery)• RFC3810 (Multicast Listener Discovery version 2 (MLDv2) for IPv6)• RFC2711 (Router-Alert option)• RFC5095 (Deprecation of Type 0 Routing Headers in IPv6)• RFC3315 (DHCPv6 filtering)• RFC4862 IPv6 Stateless Address Autoconfiguration• OSPFv3: RFC5340, RFC4552 y RFC 5838• IEEE 802.1s• IEEE 802.1w• IEEE 802.1x• IEEE 802.3ad• IEEE 802.3af• IEEE 802.3at• IEEE 802.3x full dúplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports• IEEE 802.1D Spanning Tree Protocol• IEEE 802.1p CoS prioritization• IEEE 802.1Q VLAN• IEEE 802.3u 100BASE-TX specification• IEEE 802.3ab 1000BASE-T specification• IEEE 802.3z 1000BASE-X specification.
18	Soporte de 802.1X, MACsec-256 o MACsec AES 256. Debe soportar funcionalidades de seguridad que permitan detectar amenazas en la red, tales como ataques de comando y control, ransomware, DDoS, malware desconocido, y amenazas internas, incluso si se producen sobre tráfico cifrado.
19	El equipo debe poderse montar en racks de 19 pulgadas e incluir los herrajes para su montaje.
20	El equipo debe ser administrado a través de: CLI, WEB, SNMP, SSH.
21	Debe tener luces indicadoras de múltiples funciones como estado del equipo y estado de puertos
22	El equipo debe contar con mínimo dos (2) fuentes de poder y deben ser hotswap. Alimentadas en un margen de 110VAC - 220 VAC. La potencia suministrada con las dos (2) fuentes debe ser de mínimo 1100W para la tecnología PoE.
23	El MTBF ofrecido por el fabricante debe ser como mínimo de 200000 h
24	Los equipos deben soportar e incluir funciones de programabilidad por medio de scripting en Python y soporte de APIs (Application Programmable Interfaces)



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 48 PTS MULTIGIGABIT	
Ítem	Descripción
25	Debe estar en capacidad de soportar e incluir los siguientes protocolos de gestión y automatización: NETCONF y/o YANG, ZTP y/o Open PnP y/o equivalente que permita realizar implementación automática de dispositivos de red (Switch) desde un controlador SDN.
26	Los equipos deben estar en capacidad de formar un fabric tipo SDN por medio de la virtualización de la red con mecanismos de EVPN con VXLAN.
27	Los equipos deben soportar las siguientes funcionalidades tipo SDN: <ul style="list-style-type: none">• Implementación automatizada tipo Zero-Touch• Visibilidad de endpoints y usuarios para funciones de troubleshooting: Analíticas y Telemetría.• Políticas de segmentación y microsegmentación basadas en grupos de objetos (IPv4 e IPv6).• Soportar la integración con un controlador tipo SDN que simplifique la administración y orquestación de la solución.
28	Debe incluir cable y accesorios para apilamiento de mínimo 1 metro.
29	Licenciamiento necesario para la integración a las plataformas Cisco® DNA, Cisco® NAC (ISE).

Tabla 3. Requerimientos técnicos Switch acceso 48P Multigigabit

5.3.2. Switch acceso POE

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 48 PTS POE	
Ítem	Descripción
1	Debe tener mínimo 48 puertos Non-Blocking para conector RJ-45 autosensing 10/100/1000 o 100/1000 MDIX.
2	Debe tener mínimo 4 puertos de uplink a 10G SFP+ para uplinks de alta velocidad
3	Deben soportar configuraciones de apilamiento de mínimo 8 equipos (entre Switches de Acceso de la misma familia) y se debe tener gestión de los mismos por medio de una única dirección ip
4	Debe soportar los siguientes protocolos: <ul style="list-style-type: none">• OSPFv3• VRRPv3• BGPv4• ARP• IGMPv3• SNMPv3• DHCP Server• DHCP relay



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 48 PTS POE	
Ítem	Descripción
	<ul style="list-style-type: none">• NTP• Enrutamiento estático• Enrutamiento virtual (VRF)• EVPN con VXLAN• SSH v2• ACL (IPv4 e IPv6)
5	DRAM mínima 8GB
6	FLASH mínimo 16GB
7	El equipo debe ser “ <i>non-blocking</i> ”, esto es, que la matriz de conmutación permita simultáneamente el manejo de todos los puertos a su máxima capacidad full dúplex sin bloquearse o sin presentar sobresubscripción, es decir que el equipo soporte mínimo 240 Gbps en switching capacity, sin contar el throughput del módulo físico de stack.
8	El switching capacity del stacking debe ser físico de mínimo 700 Gbps, que permita tener hasta 8 miembros.
9	Soportar mínimo 32.000 direcciones MAC
10	Soportar mínimo 32000 rutas IPv4 ARP plus learned routes) – (24,000 directas y 8,000 indirectas)
11	Soportar mínimo 16000 rutas de enrutamiento en IPv6
12	Soporte de Dual stack para IPv4/IPv6
13	Soporte de IPv6 y enrutamiento IPv6 en hardware, ya que se requiere desempeño sin sobresuscripción para tráfico y servicios IPv6.
14	Soportar mínimo 4000 VLAN ID
15	Debe soportar Jumbo frame mínimo de 9100 bytes
16	Debe soportar tasa mínima de reenvío de paquetes (Forwarding Rate) de 180 Mpps.
17	Debe cumplir con los siguientes RFC, funcionalidades y estándares: <ul style="list-style-type: none">• RFC2460 (IPv6 Basic specification)• RFC4291 (IPv6 Addressing Architecture)• RFC3484 (Default Address Selection)• RFC4193 (Unique Local IPv6 Unicast Addresses (ULA))• RFC4443 (ICMPv6)• RFC4862 (SLAAC)• RFC1981 (Path MTU Discovery)• RFC4861 (Neighbor Discovery)• RFC3810 (Multicast Listener Discovery version 2 (MLDv2) for IPv6)• RFC2711 (Router-Alert option)• RFC5095 (Deprecation of Type 0 Routing Headers in IPv6)• RFC3315 (DHCPv6 filtering)• RFC4862 IPv6 Stateless Address Autoconfiguration• OSPFv3: RFC5340, RFC4552 y RFC 5838



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 48 PTS POE	
Ítem	Descripción
	<ul style="list-style-type: none">• IEEE 802.1s• IEEE 802.1w• IEEE 802.1x• IEEE 802.3ad• IEEE 802.3af• IEEE 802.3at• IEEE 802.3x full dúplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports• IEEE 802.1D Spanning Tree Protocol• IEEE 802.1p CoS prioritization• IEEE 802.1Q VLAN• IEEE 802.3u 100BASE-TX specification• IEEE 802.3ab 1000BASE-T specification• IEEE 802.3z 1000BASE-X specification.
18	Soporte de 802.1X, MACsec-256 o MACsec AES 256. Debe soportar funcionalidades de seguridad que permitan detectar amenazas en la red, tales como ataques de comando y control, ransomware, DDoS, malware desconocido, y amenazas internas, incluso si se producen sobre tráfico cifrado.
19	El equipo debe poderse montar en racks de 19 pulgadas e incluir los herrajes para su montaje.
20	El equipo debe ser administrado a través de: CLI, WEB, SNMP, SSH.
21	Debe tener luces indicadoras de múltiples funciones como estado del equipo y estado de puertos
22	El equipo debe contar con mínimo dos (2) fuentes de poder y deben ser hotswap. Alimentadas en un margen de 110VAC - 220 VAC. La potencia suministrada con las dos (2) fuentes debe ser de mínimo 1100W para la tecnología PoE.
23	El MTBF ofrecido por el fabricante debe ser como mínimo de 270000 h
24	Los equipos deben soportar e incluir funciones de programabilidad por medio de scripting en Python y soporte de APIs (Application Programmable Interfaces)
25	Debe estar en capacidad de soportar e incluir los siguientes protocolos de gestión y automatización: NETCONF y/o YANG, ZTP y/o Open PnP y/o equivalente que permita realizar implementación automática de dispositivos de red (Switch) desde un controlador SDN.
26	Los equipos deben estar en capacidad de formar un fabric tipo SDN por medio de la virtualización de la red con mecanismos de EVPN con VXLAN.
27	Los equipos deben soportar las siguientes funcionalidades tipo SDN: <ul style="list-style-type: none">• Implementación automatizada tipo Zero-Touch• Visibilidad de endpoints y usuarios para funciones de troubleshooting: Analíticas y Telemetría.• Políticas de segmentación y microsegmentación basadas en grupos de objetos (IPv4 e IPv6).



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 48 PTS POE	
Ítem	Descripción
	<ul style="list-style-type: none">• Soportar la integración con un controlador tipo SDN que simplifique la administración y orquestación de la solución.
28	Debe incluir cable y accesorios para apilamiento de mínimo 1 metro.
29	Licenciamiento necesario para la integración a las plataformas Cisco® DNA, Cisco® NAC (ISE).

Tabla 4. Requerimientos técnicos Switch acceso 48P POE

5.3.3. Switch acceso Data

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 48 PTS DATA	
ítem	Descripción
1	Debe tener mínimo 48 puertos Non-Blocking para conector RJ-45 autosensing 10/100/1000 o 100/1000 MDIX.
2	Debe tener mínimo 4 puertos de uplink a 10G SFP+ para uplinks de alta velocidad
3	Deben soportar configuraciones de apilamiento de mínimo 8 equipos (entre Switches de Acceso de la misma familia) y se debe tener gestión de los mismos por medio de una única dirección ip
4	Debe soportar los siguientes protocolos: <ul style="list-style-type: none">• OSPFv3• VRRPv3• BGPv4• ARP• IGMPv3• SNMPv3• DHCP Server• DHCP relay• NTP• Enrutamiento estático• Enrutamiento virtual (VRF)• EVPN con VXLAN• SSH v2• ACL (IPv4 e IPv6)
5	DRAM mínima 8GB
6	FLASH mínimo 16GB
7	El equipo debe ser “ <i>non-blocking</i> ”, esto es, que la matriz de conmutación permita simultáneamente el manejo de todos los puertos a su máxima capacidad full dúplex sin bloquearse o sin presentar sobresubscripción, es decir que el equipo



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 48 PTS DATA	
ítem	Descripción
	soporte mínimo 230 Gbps en switching capacity, sin contar el throughput del módulo físico de stack.
8	El switching capacity del stacking debe ser físico de mínimo 700 Gbps, que permita tener hasta 8 miembros.
9	Soportar mínimo 32.000 direcciones MAC
10	Soportar mínimo 32000 rutas IPv4 ARP plus learned routes) – (24,000 directas y 8,000 indirectas)
11	Soportar mínimo 16000 rutas de enrutamiento en IPv6
12	Soporte de Dual stack para IPv4/IPv6
13	Soporte de IPv6 y enrutamiento IPv6 en hardware, ya que se requiere desempeño sin sobresuscripción para tráfico y servicios IPv6.
14	Soportar mínimo 4000 VLAN ID
15	Debe soportar Jumbo frame mínimo de 9100 bytes
16	Debe soportar tasa mínima de reenvío de paquetes (Forwarding Rate) de 180 Mpps.
17	<p>Debe cumplir con los siguientes RFC, funcionalidades y estándares:</p> <ul style="list-style-type: none">• RFC2460 (IPv6 Basic specification)• RFC4291 (IPv6 Addressing Architecture)• RFC3484 (Default Address Selection)• RFC4193 (Unique Local IPv6 Unicast Addresses (ULA))• RFC4443 (ICMPv6)• RFC4862 (SLAAC)• RFC1981 (Path MTU Discovery)• RFC4861 (Neighbor Discovery)• RFC3810 (Multicast Listener Discovery version 2 (MLDv2) for IPv6)• RFC2711 (Router-Alert option)• RFC5095 (Deprecation of Type 0 Routing Headers in IPv6)• RFC3315 (DHCPv6 filtering)• RFC4862 IPv6 Stateless Address Autoconfiguration• OSPFv3: RFC5340, RFC4552 y RFC 5838• IEEE 802.1s• IEEE 802.1w• IEEE 802.1x• IEEE 802.3ad• IEEE 802.3af• IEEE 802.3at• IEEE 802.3x full dúplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports• IEEE 802.1D Spanning Tree Protocol• IEEE 802.1p CoS prioritization



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

REQUERIMIENTOS TÉCNICOS SWITCH DE ACCESO 48 PTS DATA	
ítem	Descripción
	<ul style="list-style-type: none">• IEEE 802.1Q VLAN• IEEE 802.3u 100BASE-TX specification• IEEE 802.3ab 1000BASE-T specification• IEEE 802.3z 1000BASE-X specification.
18	Soporte de 802.1X, MACsec-256 o MACsec AES 256. Debe soportar funcionalidades de seguridad que permitan detectar amenazas en la red, tales como ataques de comando y control, ransomware, DDoS, malware desconocido, y amenazas internas, incluso si se producen sobre tráfico cifrado.
19	El equipo debe poderse montar en racks de 19 pulgadas e incluir los herrajes para su montaje.
20	El equipo debe ser administrado a través de: CLI, WEB, SNMP, SSH.
21	Debe tener luces indicadoras de múltiples funciones como estado del equipo y estado de puertos
22	El equipo debe contar con mínimo dos (2) fuentes de poder de mínimo 350 W cada una y deben ser hotswap. Alimentadas en un margen de 110VAC - 220 VAC
23	El MTBF ofrecido por el fabricante debe ser como mínimo de 298000 h
24	Los equipos deben soportar e incluir funciones de programabilidad por medio de scripting en Python y soporte de APIs (Application Programmable Interfaces)
25	Debe estar en capacidad de soportar e incluir los siguientes protocolos de gestión y automatización: NETCONF y/o YANG, ZTP y/o Open PnP y/o equivalente que permita realizar implementación automática de dispositivos de red (Switch) desde un controlador SDN.
26	Los equipos deben estar en capacidad de formar un fabric tipo SDN por medio de la virtualización de la red con mecanismos de EVPN con VXLAN.
27	Los equipos deben soportar las siguientes funcionalidades tipo SDN: <ul style="list-style-type: none">• Implementación automatizada tipo Zero-Touch• Visibilidad de endpoints y usuarios para funciones de troubleshooting: Analítica y Telemetría.• Políticas de segmentación y microsegmentación basadas en grupos de objetos (IPv4 e IPv6).• Soportar la integración con un controlador tipo SDN que simplifique la administración y orquestación de la solución.
28	Debe incluir cable y accesorios para apilamiento de mínimo 1 metro.
29	Licenciamiento necesario para la integración a las plataformas Cisco® DNA, Cisco® NAC (ISE).

Tabla 5. Requerimientos técnicos Switch acceso 48P Data

5.4. Requerimientos técnicos módulo transceiver



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

REQUERIMIENTOS TÉCNICOS MODULO TRANSCEIVER SFP	
Ítem	Descripción
1	Longitud de onda: 850nm
2	Máxima tasa de transferencia de datos: 10Gbps
3	Tipo: Fibra óptica MULTIMODO 50/125um
4	Tipo de conexión: Conector LC
5	Distancia máxima de transferencia: 400m
6	Consumo energético: 1 vatio
7	Transceiver form factor SFP+
8	Debe admitir intercambio en caliente, lo cual facilita las actualizaciones y reemplazos, ya que minimiza las interrupciones de conexión en red.
9	Deben ser originales y aprobados por el fabricante para operar con la solución de Networking en donde se instalarán.

Tabla 6. Requerimientos técnicos módulo transceiver SFP+

6. REQUERIMIENTOS TÉCNICOS NETWORKING WLAN

- a. Suministrar los Access Point, incluyendo su respectivo licenciamiento, soporte, garantía, módulos y accesorios, en cumplimiento de las condiciones técnicas exigidas.
- b. El proponente debe contemplar los pasamuros, pasaplacas y perforaciones pertinentes para la correcta instalación de los Access Point.
- c. Toda instalación de hardware y software debe ser realizada por personal certificado de fábrica. Durante la ejecución del contrato se deben suministrar los soportes que permitan verificar este requerimiento.
- d. Todos los Access Point deberán integrarse con la controladora WLC Cisco 9800 así como con el appliance Cisco® DNA (Digital Network Architecture) versión 2.3.7.7 y el controlador de acceso a la red Cisco® ISE (Identity Services Engine) a efectos de aprovechar los recursos, tecnologías y plataformas de administración de la Universidad, por lo tanto, el proponente debe suministrar las licencias advantage necesarias para los equipos Access point indoor y outdoor sobre la plataforma DNA y controladora WLC, las cuales deben estar contempladas en la oferta económica.

6.1. Access point indoor

REQUERIMIENTOS TÉCNICOS ACCESS POINT INDOOR	
Ítem	Descripción
1	Debe cumplir los estándares de comunicación Wifi a/b/g/n/ac/ax
2	Debe funcionar en las bandas de frecuencia 2.4 GHz, 5 GHz y 6 GHz.



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

REQUERIMIENTOS TÉCNICOS ACCESS POINT INDOOR	
Ítem	Descripción
3	Debe soportar mínimo el siguiente ancho de banda en los siguientes estándares: <ul style="list-style-type: none">• 802.11be• 802.11ax• 802.11ac• 802.11n versión 2.0
4	Debe soportar IPv4, IPv6, dual-stack a nivel de hardware y software.
5	La cobertura del AP debe ser omnidireccional.
6	Debe contar mínimo con la tecnología MU-MIMO 4X4 Spatial Streams.
7	Debe soportar beamforming o beamflex
8	Debe contar con antenas internas únicamente
9	Debe poder realizar un análisis de espectro de RF avanzado a través del Access Point o mediante la Controladora Inalámbrica con el fin de aprovechar tecnologías como Wireless Intrusion Prevention System (wIPS) y Dynamic Frequency Selection o ChannelFly.
10	Debe ser administrable por CLI (SSH), SNMPv1, 2, 3 y Vía equipo Controlador.
11	Debe soportar alimentación PoE sobre el estándar 802.3at.
12	Debe contar con mínimo un (1) puerto RJ-45 auto MDI/X, auto-sensing (100/1000/2500/5000 BASE-T)
13	Rango de temperaturas mínimas en operación 0°C a 50°C
14	Condiciones de humedad mínimas 10% a 90% sin condensación (noncondensing)
15	Debe soportar WPA, WPA2, WPA3
16	Debe cumplir con la certificación generada por la WIFI ALLIANCE para Wi-Fi 7 (R1), Wi-Fi 6 (R2), Wi-Fi 6E, WPA3-R3, WPA3-Suite B, Enhanced Open Security
17	Licenciamiento necesario para la integración a las plataformas Cisco® DNA, Cisco® NAC (ISE).

Tabla 7. Requerimientos técnicos Access Point Indoor

6.2. Access point outdoor

REQUERIMIENTOS TÉCNICOS ACCESS POINT OUTDOOR	
Ítem	Descripción
1	Debe cumplir los estándares de comunicación Wifi a/b/g/n/ac/ax
2	Debe funcionar en las bandas de frecuencia 2.4 GHz y 5 GHz
3	Debe soportar mínimo el siguiente ancho de banda en los siguientes estándares: <ul style="list-style-type: none">• 802.11n versión 2.0• 802.11ac• 802.11ax



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

REQUERIMIENTOS TÉCNICOS ACCESS POINT OUTDOOR	
Ítem	Descripción
4	Debe soportar IPv4, IPv6
5	La cobertura del AP debe ser omnidireccional.
6	Debe contar mínimo con la tecnología MU-MIMO 4X4
7	Debe soportar beamforming o beamflex
8	Debe contar con cuatro (4) antenas externas
9	Debe poder realizar un análisis de espectro de RF avanzado a través del Access Point o mediante la Controladora Inalámbrica con el fin de aprovechar tecnologías como Wireless Intrusion Prevention System (wIPS) y Dynamic Frequency Selection o ChannelFly.
10	Debe ser administrable por CLI (SSH), SNMPv1, 2, 3 y Vía equipo Controlador
11	Debe soportar alimentación PoE sobre el estándar 802.3at
12	Debe contar con mínimo un (1) puerto RJ-45 auto MDI/X, auto-sensing (100/1000/2500 BASE-T)
13	Rango de temperaturas mínimas -40°C a 65°C
14	Condiciones de humedad mínimas 0% a 100% con condensación (condensing)
15	Debe soportar el estándar IP67
16	Debe soportar WPA, WPA2, WPA3
17	Debe cumplir con la certificación generada por la WIFI ALLIANCE para Wi-Fi 6
18	Licenciamiento necesario para la integración a las plataformas Cisco® DNA, Cisco® NAC (ISE).

Tabla 8. Requerimientos técnicos Access Point outdoor

7. REQUERIMIENTOS DE DESEMPEÑO

Los equipos a adquirir deberán cumplir como mínimo las siguientes condiciones:

- **Alta disponibilidad de hardware:** Los equipos switches deberán garantizar una disponibilidad mínima del 99,9 %, basada en componentes de hardware redundantes (fuentes de poder y ventiladores)
- **Soporte técnico y niveles de servicio (SLA):** El proveedor deberá garantizar un servicio de soporte técnico especializado 8x5xNBD para el hardware. Los tiempos de respuesta ante fallas de hardware deberán estar acorde a la criticidad del incidente, incluyendo el reemplazo de componentes críticos (partes y piezas) en sitio, asegurando la continuidad de los servicios.



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

8. PRUEBAS Y CRITERIOS DE ACEPTACIÓN

- El proponente debe acreditar que, para este proceso de contratación, cuenta con el respaldo del fabricante de los bienes, hardware, software y componentes, anexando un documento expedido directamente por el fabricante, en el que certifique que es partner, el cual está autorizado y en capacidad de instalar, configurar y soportar los equipos adquiridos en presente proceso. Dicho certificado deberá estar vigente durante la validez de la propuesta. De igual manera durante la ejecución del contrato, el contratista debe contar con la certificación de partner vigente.
- El partner debe tener vigente la especialización: Advanced Security Architecture Specialization y Advanced Enterprise Networks Architecture Specialization expedida por fabricante, con el fin de asegurar la correcta integración entre las plataformas NAC (ISE), DNA y los equipos de red propiedad de la Universidad.
- El partner debe tener vigente la especialización: Advanced Customer Experience Specialization con el fin de asegurar el conocimiento de experiencia al cliente en la adopción de soluciones DNA y los equipos de red propiedad de la Universidad.
- Certificación del fabricante donde se garantiza que los equipos y sus componentes se encuentran registrados ante el fabricante.
- El contratista debe entregar carta o certificación expedida por el fabricante, a nombre de la Universidad Distrital Francisco José de Caldas, en donde se discrimine la cobertura y la duración del soporte que ampara a los equipos.

Para el desarrollo del proyecto se solicita la siguiente documentación técnica:

- Presentar y ejecutar el cronograma de instalación, configuración y pruebas, este cronograma debe actualizarse cada vez que las fechas se cumplan.
- Presentar un protocolo para la verificación de la configuración y la ejecución de pruebas (checklist).
- Realizar el levantamiento de información de la topología de red, así como de las políticas y configuraciones de los equipos actuales.
- Realizar site survey previo a la instalación de los Access Point, para identificar la ubicación óptima de los Access Point para el despliegue de la red Wifi.
- Entregar el Site Survey (mapa de calor) generado por los Access Point una vez se encuentren instalados y en funcionamiento, este deberá tener en cuenta la arquitectura de las sedes.



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

- El contratista debe entregar documento descriptivo y con topología física y lógica de la implementación de la solución, donde se mencionen velocidades, equipos y protocolos.
- Es responsabilidad del contratista diligenciar y elaborar las actas de asistencia y de las sesiones de seguimiento del contrato, las cuales serán aprobadas por el supervisor del contrato.
- El personal que realice la instalación de los Access point debe contar con certificado de trabajo de alturas vigente, el cual será verificado por el subsistema de gestión de la seguridad y salud en el trabajo de la Universidad.

9. GARANTÍA Y SOPORTE

El soporte a contratar debe ser de partner con certificación vigente de la marca de los equipos, este soporte iniciará a partir de la entrega de los equipos en correcto funcionamiento, con las respectivas pruebas de arranque y recibo a satisfacción por parte del supervisor, debe incluir la última versión oficial y estable del software y firmware, lo cual debe ser realizado por el personal técnico certificado por el fabricante. Por lo tanto, el contratista debe asegurar que cuenta con este personal en cumplimiento de términos y condiciones establecidas por la Universidad.

9.1. Soporte

Todas las actividades y procedimientos que conlleven a la atención de requerimientos técnicos solicitados a los equipos LAN y WLAN, para atender eventos o incidencias que se presenten.

Se debe contar con los siguientes niveles de atención durante el periodo de la duración del contrato:

- Atención telefónica y/o atención vía correo electrónico a través de Centro de atención de llamadas o de medios electrónicos: Atención telefónica y/o de correo electrónico inmediata en esquema 8X5XNBD para reportar la falla.
- Atención remota: Soporte remoto en horario hábil bajo modalidad 8X5XNBD, a partir de las 8:00 a.m.
- Atención en sitio: Soporte en sitio en horario hábil bajo modalidad 8X5XNBD, a partir de las 8:00 a.m.
- Registro de número de incidentes ante partner y fabrica: Para cualquier tipo de soporte se debe generar ticket del incidente tanto del partner como de fábrica, para verificación del estado y seguimiento del mismo por parte de la Universidad Distrital Francisco José de caldas



UNIVERSIDAD DISTRICTAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

9.2. Procedimiento de mantenimiento

El contratista, máximo cinco (5) días hábiles después de firmada el acta de inicio debe enviar al correo de la supervisión el plan de mantenimiento, en el cual se definen procedimientos y actividades a ejecutar de acuerdo con las recomendaciones del fabricante. Este documento debe ser aprobado por la supervisión. Todo procedimiento deberá ser acordado y contar con el acompañamiento del personal que la supervisión designe.

9.3. Mantenimiento preventivo

Se entiende por mantenimiento preventivo, las estrategias que pretenden maximizar la vida útil y operativa de los equipos switches y sus componentes, identificando las posibles causas que pueden originar fallas futuras e indicando las medidas a tomar para evitarlas.

Durante la ejecución del contrato, se deben realizar una (1) rutina de mantenimiento preventivo por año, la cual debe ser coordinada previamente con la supervisión y que incluya como mínimo:

- Backup de la configuración.
- Revisión de puertos y tarjetas.
- Backup y verificación de registros sobre eventos y/o alarmas.
- Diagnóstico de registros sobre eventos y/o alarmas.
- Apagado de acuerdo a manuales.
- Mantenimiento preventivo a hardware (físico)
- Actualización de software y firmware si aplica, en caso de presentar problemas en el desempeño se debe revertir el parche o firmware que se instaló y se debe conservar la versión que garantice el correcto funcionamiento.
- Revisiones generales.
- Puesta en correcto funcionamiento y verificación de servicios.

9.4. Mantenimiento Correctivo

Se entiende por mantenimiento correctivo, todas las actividades y procedimientos que conlleve a la solución de las fallas que se presenten en la infraestructura descrita en el



UNIVERSIDAD DISTRICTAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

presente documento, como también la solución de estas y la puesta en operación normal del equipo y sus componentes.

El mantenimiento correctivo puede derivar de un mantenimiento preventivo en el que se evidencia una falla o de una falla detectada y reportada por el equipo técnico de la Red de Datos de la Universidad Distrital.

El contratista puede realizar el diagnóstico de la falla de manera remota, de no ser posible, debe enviar un ingeniero al sitio donde se encuentra ubicado el equipo en falla en un plazo menor o igual a veinticuatro (24) horas para corregir el inconveniente o verificar la necesidad de reemplazo de la parte. (RMA).

El Tiempo máximo para reemplazo de equipos, tarjetas y partes, será de 1 día hábil después de diagnosticada la falla.

Los elementos que se requieran reemplazar deben ser nuevos, originales y ensamblados de fábrica.

9.5. Documentación soporte de actividades de mantenimiento

- El contratista debe entregar documento con el esquema de escalamiento SLA para niveles de servicio.
- Entrega en medio digital de los registros de eventos y fallas.
- Reporte de visita técnica: Se debe generar siempre que el contratista realice una visita en sitio y debe incluir como mínimo: serial del equipo, fecha, soporte y datos de contacto, líneas telefónicas, correos electrónicos, procedimientos realizados, observaciones y hallazgos.
- Informe técnico: en un plazo no mayor a cinco (5) días hábiles de realizado el mantenimiento (preventivo o correctivo), el contratista debe presentar a la supervisión del contrato el informe de las actividades realizadas, este informe debe incluir como mínimo:
 - Fecha de la actividad
 - Equipos intervenidos con su respectivo serial
 - Actividades realizadas
 - Descripción, análisis y recomendaciones resultantes de la lectura del registro de eventos y fallas presentes para los mantenimientos preventivos.
 - Diagnóstico y concepto técnico sobre la falla, causas, soluciones y recomendaciones (Si aplica)
 - Listado de seriales y denominación de partes reemplazadas y retiradas (Si aplica).



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

9.6. RMA o revisión en laboratorio del contratista

Cuando el diagnóstico sobre los equipos o partes determine falla total o parcial, el contratista deberá realizar el proceso de RMA, coordinar la logística y realizar la instalación configuración y puesta en correcto funcionamiento del equipo a reemplazar, así como la devolución del equipo o parte afectada durante el tiempo de garantía vigente.

Todo traslado de equipos y elementos estará a cargo del contratista, tanto para el retiro como para la entrega en las instalaciones de la Universidad.

En caso de falla el contratista proporcionará y dejará en funcionamiento un sustituto de iguales o superiores características y capacidades, (incluyendo sus componentes), sin que ello genere costos adicionales para la Universidad Distrital Francisco José de Caldas.

La atención de soporte y reemplazo de partes será en esquema 8x5xNBD: 5 días hábiles de la semana de 8:00 am a 5:00 pm, con remplazo de hardware al siguiente día hábil. Estos servicios hacen parte de la oferta incluyendo todos costos asociados para su cumplimiento (fletes, impuestos, transporte, importación, entre otros).

9.7. Actualización de Software (update y upgrade)

Las actualizaciones "*update*" son aquellas que se implementan para corregir errores, mejorar el rendimiento de los equipos o implementar nuevas funciones o características sin cambiar la versión principal del software, mientras que las "*upgrade*" implican una mejora o cambio sustancial, como la instalación de una versión más reciente con nuevas funciones o mejoras significativas.

El contratista, previo a la ejecución de una actualización, debe informar al correo telecomunicaciones@udistrital.edu.co el tipo de actualización a realizar, las actividades a ejecutar, el tiempo estimado que tomará la actualización y si esta causa afectación de los servicios prestados. La Unidad Red de Datos confirmará por correo electrónico la ejecución de la actualización.

Para todas las actualizaciones se deben tener en cuenta las siguientes actividades:

- Backup de la configuración.
- Revisión de puertos y tarjetas.
- Backup y verificación de registros sobre eventos y/o alarmas.
- Diagnóstico de registros sobre eventos y/o alarmas.



UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Rectoría

Unidad Red de Datos UDNET

- Apagado de acuerdo a manuales.
- Actualización de software, en caso de presentar problemas en el desempeño se debe revertir las actualizaciones de software que se instaló y se debe conservar la versión que garantice el correcto funcionamiento.
- Revisiones generales.
- Puesta en correcto funcionamiento y verificación de servicios.