

Tender Document for active and passive Optical Fiber/WiFi Networking
PGDAV College

On behalf of the Principal PGDAV College, Nehru Nagar, New Delhi, INDIA, sealed bids are invited under two bid system from reputed manufacturers or their authorized agents for the supply / installation/Testing/ Integration and commissioning of the following item/work(s): -

Items Required

1. Active Component:

S.L. No	Item description	Qty
1.1	8 port PoE Switch with required gigabit SFP modules, 5 year OEM support & warranty (Make - Ruckus commscope, Cisco, HP, Juniper)	5
1.2	12 Port PoE Switch with required gigabit SFP modules, 5 year OEM support & warranty (Make - Ruckus commscope, Cisco, HP, Juniper)	1
1.3	12 port non poe gigabit fiber switch with 10 SFP with required gigabit SFP modules 5 year OEM support & warranty (Make - Ruckus commscope, Cisco, HP & Dlink)	1
1.4	Wireless hardware controller with 5 year warranty and OEM support & supports 40 AP lic from day 1 (Make- Ruckus, Cisco, HP, Juniper)	2
1.5	Hardware controller managed 2*2:2 Indoor Wi-Fi 6 (802.11ax) Access Point with 5 year warranty and OEM support (Make- Ruckus, Cisco, HP, Juniper)	20
1.6	Hardware controller managed Indoor Wi-Fi 6 (802.11ax) 4x4:4 Wi-Fi Access Point with 2.5Gbps backhaul and 6 spatial streams with 5 year warranty and OEM support (Make- Ruckus, Cisco, HP, Juniper)	20
1.7	Hardware Firewall Supports 200-250 concurrent Users with 5 year warranty and OEM support (Make - Sophos, Netxgate & Fortinet)	1

2. Passive Component:

S.L. No	Item	Qty
2.1	Network rack 6u with all standard accessories	6
2.2	Cat6 Patch panel 24 port Unloaded (Make- R&M, Dlink, Molex)	6
2.3	Cat 6 UTP Information Outlet (Make- R&M, Dlink, Molex)	90
2.4	Cat 6 Patch Cord 2m Cat6 (Make- R&M, Dlink, Molex)	90
2.5	Cat6 305 m roll (Make- R&M, Dlink, Molex)	16
2.6	25mm conduit PVC bundle (Make - any but ISI mark)	19
2.7	Outdoor 6 core armoured MM fiber cable (in meter) (Make- R&M, Dlink, Molex)	750
2.8	Fiber LIU 6 core (Make- R&M, Dlink, Molex)	5
2.9	Fiber LIU 24 core fully loaded (Make- R&M, Dlink, Molex)	1
3	Fiber coupler MM (Make- R&M, Dlink, Molex)	30
3.1	fiber patch cord sc-LC 2m (Make- R&M, Dlink, Molex)	8

Krishna Sharma
OFFICIATING PRINCIPAL
P.G.D.A.V. COLLEGE
 Nehru Nagar, New Delhi-110065
hi

3.2	Fiber pigtail mm (Make- R&M, Dlink, Molex)	30
3.3	HDPE pipe 25mm ISI mark (in metre) (Make - any but ISI mark)	800

3. Service Component:

4.1	Fibre splicing as required with OTDR testing - one time - lumpsum	1
4.2	One time Cable laying with conduiting - Lumpsum	1
4.3	One time Rack fitting, Patchpanel, switch installation - Lumpsum	1
4.4	One time Cat6 Patch panel punching (rack side only) Lumpsum for all and new Patch panels	1
4.5	One time Controller, AP, P2P, Firewall installation & configuration - Lumpsum for all Active devices	1
4.6	One time Fibre laying service (machinery, tools, earth digging, fiber, HDPE / conduit laying, civil work with necessary civil material) -	1

Technical Specification for Active Component

1.1 Specifications for Switch with 8 1G PoE RJ45 ports and 2 1G SFP slots:

Sl. No	Specification Required	Compliance Yes / No	Remarks
1.0	Product details- Please specify		
1.1	Please mention Make, Model No. and Part Code		
2.0	Architecture & Port Density		
2.1	The Switch should offer Wire-Speed Non-Blocking Switching & Routing Performance at Layer 2 & Layer 3.		
2.2	The Switch should have minimum Eight (8) 1G PoE RJ45 ports and should have Two (2) 1G SFP Slots, from Day 1.		
3.0	Performance		
3.1	Switching Bandwidth: Should provide Non-Blocking switch fabric capacity of 20 Gbps or more.		
3.2	Forwarding Capacity: Should provide wire-speed packet forwarding of 14.88 Mpps or more.		
4.0	Layer 2 features		
4.1	Should support 1K VLANs with 4K VLAN IDs		
4.2	Should support 8K MAC addresses or more.		
4.3	Shall support IP multicast snooping with support for IGMP v1, v2, v3 and MLD v1 & v2		

Krishna Shermu
 OFFICIATING PRINCIPAL
 P.G.D.A.V. COLLEGE
 Nehru Nagar, New Delhi-110085

4.4	Should support Jumbo Frames (up to 9K bytes)		
5.0	<u>Security</u>		
5.1	Switch should support RADIUS, TACACS/TACACS+ and username/password for Authentication, Authorization and Accounting (AAA) with Local User Accounts and Local User Passwords.		
5.2	Should support secure communications to the management interface and system through SSL, Secure Shell (SSHv2), Secure Copy and SNMPv3		
5.3	Should support Byte and packet based broadcast, multicast, and unknown-unicast limits with suppression port dampening.		
5.4	Should support Flexible Authentication with 802.1x Authentication and MAC Authentication.		
6.0	<u>Manageability</u>		
6.1	Should support manageability using Network Management Software with Web based Graphical User Interface (GUI).		
6.2	Integrated Standard based Command Line Interface (CLI), Telnet, TFTP, HTTP access to switch management/monitoring		
6.3	Should support NetFlow or sFlow or equivalent		
7.0	<u>Physical Attributes & PoE Power Budget</u>		
7.1	Mounting Option: The Switch should be configured with 19" Universal rack mount kit.		
7.2	PoE Power Budget: The PoE Switch should provide a minimum of 60 watts of PoE+ power.		
8.0	<u>Mandatory Compliance</u>		
8.1	All categories of Switches, Transceivers & Switch OS should be from same OEM		
9.0	<u>Warranty</u>		
9.1	The Switch should be quoted with TAC Support and Warranty for 3 years with NBD Hardware Replacement.		
10.0	<u>Product brochure</u> Vendor should provide printed technical catalogs/brochures for the quoted model containing technical specifications, features.		

Kishor sharma
OFFICIATING PRINCIPAL
P.G.D.A.V. COLLEGE
 Nehru Nagar, New Delhi-110065

[Signature]

1.2 Technical specifications of PoE Access Switch, with 2 x 10G SFP+ Slots & 12 x 1G PoE+ RJ45

Ports:

Sl. No	Specification Required	Compliance Yes / No	Remarks
1.0	<u>Product details- Please specify</u>		
1.1	Please mention Make, Model No. and Part Code		
2.0	<u>Architecture & Port Density</u>		
2.1	The Access Switch should offer Wire-Speed Non-Blocking Switching & Routing Performance at Layer 2 & Layer 3.		
2.2	The Access Switch should have Two (2) 10GbE SFP Slots and Twelve (12) 1GbE PoE RJ45 ports.		
2.3	The Access Switch should support Stacking up to 8 Switches.		
3.0	<u>Performance</u>		
3.1	Switching Bandwidth: Should provide Non-Blocking switch fabric capacity of 64 Gbps or more.		
3.2	Forwarding Capacity: Should provide wire-speed packet forwarding of 47 Mpps or more.		
4.0	<u>Layer 2 features</u>		
4.1	Switch should support 4K Active VLANs		
4.2	Switch should support 10K MAC addresses or more.		
4.3	Switch should support IP multicast snooping with support for IGMP v1, v2, v3 and MLD v1 & v2		
4.4	Switch should support Jumbo Frames (up to 9K bytes)		
5.0	<u>Layer 3 features</u>		
5.1	Switch should support minimum 1K IPv4 Routes or more		
5.2	Switch should support Basic IPv4 and IPv6 Static Routing, ECMP, Host Routes, Virtual Interfaces, Routed Interfaces, Route Only and Routing between directly connected subnets from Day 1.		
5.3	Switch should support Dynamic IPv4 & IPv6 Routing protocols (OSPFv2 and OSPFv3) and Layer 3 Multicast Routing Protocols in future, with a license upgrade.		
6.0	<u>Security</u>		

Krishna Sharma
OFFICIATING PRINCIPAL
P.G.D.A.V. COLLEGE
Nehru Nagar, New Delhi-110065



6.1	Switch should support RADIUS, TACACS/TACACS+ and username/password for Authentication, Authorization and Accounting (AAA) with Local User Accounts and Local User Passwords.		
6.2	Switch should support secure communications to the management interface and system through SSL, Secure Shell (SSHv2), Secure Copy and SNMPv3		
6.3	Switch should support IP Source Guard, DHCP snooping, DHCPv4, DHCPv6 and Dynamic ARP Inspection.		
6.4	Switch should support IPv4 and IPv6 ACLs with up to 500 rules per ACL and a minimum of 6K rules per system (Standalone Switch or Stack).		
6.5	Switch should support Byte and packet based broadcast, multicast, and unknown-unicast limits with suppression port dampening.		
6.6	Switch should support IPv6 Router Advertisement (RA) Guard.		
6.7	Switch should support Flexible Authentication with 802.1x Authentication and MAC Authentication.		
7.0	<u>Manageability</u>		
7.1	Switch should support manageability using Network Management Software with Web based Graphical User Interface (GUI).		
7.2	Switch should provide Integrated Standard based Command Line Interface (CLI), Telnet, TFTP, HTTP access to switch management/monitoring		
7.3	Switch should support NetFlow or sFlow or equivalent		
8.0	<u>Physical Attributes & PoE Power Budget</u>		
8.1	Mounting Option: 19" Universal rack mount ears		
8.2	PoE Power Budget: The Switch should provide a minimum of 120 watts of PoE+ power.		
9.0	<u>Mandatory Compliance :</u>		
9.1	All categories of Switches, Transceivers & Switch OS should be from same OEM		
10.0	<u>Warranty</u>		
10.1	Switch should be quoted with TAC Support and Warranty for 3 years with NBD Hardware Replacement.		
11.0	<u>Product brochure</u>		
	Vendor should provide printed technical catalogs/brochures for the quoted model containing technical specifications, features.		

Krishna Sharma
 OFFICIATING PRINCIPAL
 P.G.D.A.V. COLLEGE
 Nehru Nagar, New Delhi-110065

[Signature]

1.3 Access Switch with 12-Port Gigabit Fiber Ethernet Switch

Sl. No	Specification Required	Compliance Yes / No	Remarks
2.0	<u>Architecture & Port Density</u>		
2.1	The Access Switch should offer 10 x SFP ports		
2.2	The Access Switch should have 2 x 10/100/1000BASE-T ports		
2.3	The Access Switch should support Comprehensive Layer 2 features including Link Aggregation, Port-based Q-in-Q, and VLAN trunking		
2.4	The Access Switch should support Enhanced network security with IP-MAC Port-Binding (IMPB), Access Control List (ACL), and IEEE 802.1X		
2.5	The Access Switch should support Embedded 6 kV surge protection, sub-50 ms recovery ERPS, and Dying Gasp provide optimal reliability		
	<u>Warranty</u>		
3.1	Switch should be quoted with TAC Support and Warranty for 3 /5 years with NBD Hardware Replacement.		
3.2	<u>Product brochure</u>		
	Vendor should provide printed technical catalogs/brochures for the quoted model containing technical specifications, features.		

1.4 Wireless Controller Specifications:

	Description	Compliance (Yes/No)
	Essential Features:	
1	Controller should be 19" Rack mountable 1U/2U height.	
2	WLAN Controller should have minimum 2 nos. of 10/100/1000 Ethernet or SFP Ports and one Console port.	
3	Proposed Controller support up to 150 AP on a single hardware with support of seamless roaming access over L2/L3 network.	
5	Controller should support minimum 250 WLAN's	

Krishna Sharma
 OFFICIATING PRINCIPAL
 P.G.D.A.V. COLLEGE
 Nehru Nagar, New Delhi-110065



6	Controller should have capacity to handle minimum 4000 or more Concurrent devices.	
	General Feature	
7	Controller should provide air-time fairness between these different speed clients – slower clients should not be starved by the faster clients and faster clients should not adversely affected by slower clients.	
8	Controller should support Spectrum Analysis feature to detect interference from different sources.	
9	System Should provide real-time charts showing interference for access point, on a per-radio, per-channel basis.	
10	Ability to map SSID to VLAN and dynamic VLAN support for same SSID.	
11	support automatic channel selection for interference avoidance	
12	Controller must support 802.11k and 802.11r.	
	Auto Deployment of AP's at different locations	
13	Access points can discover controllers on the same L2 domain without requiring any configuration on the access point.	
14	Access points can discover controllers across Layer-3 network through DHCP or DNS option	
	Security & monitoring	
15	Controller should support following for security & Authentication:	
16	WIRELESS SECURITY: WEP, WPA-TKIP, WPA2-AES, WPA3, 802.11i	
17	AUTHENTICATION : 802.1X, local database External AAA servers : Active Directory, RADIUS, LDAP	
18	System should provide DOS attacks and Intrusion Detection & Prevention and Control for any Rouge Access Points.	
19	The AP should be able to scan for rogue access points and the controller should be able to locate them on a floor map. The controller should be able to send a notification to the administrator when a rogue AP has been detected.	
20	Controller should support CAPWAP/LWAPP protocol.	
21	System must be able to provide L2/L3/L4 Access Control.	

Krishna Shorma
 OFFICIATING PRINCIPAL
 P.G.D.A.V. COLLEGE
 Nehru Nagar, New Delhi-110065

41

22	Controller Should support L2 Client Isolation so User cannot access each other's devices. Isolation should have option to apply on AP or SSID's.	
23	Controller should be able to create local database of up to 4000 users.	
24	Controller should support Access Control based on Identity/Role/ Device/time or Application.	
25	Support for Walled garden "Walled Garden" functionality to allow restricted access to select destinations by unauthorized wireless users.	
26	IPv4 & IPv6 support from Day 1	
27	Should support on board and external DHCP server	
28	Controller should support integrated or External AAA server including Microsoft AD and Linux based open source AAA servers.	
29	The proposed architecture should be based on controller based Architecture with thick AP deployment. While Encryption / decryption of 802.11 packets should be able to perform at the AP.	
30	The Controller should support OS/Device finger printing and device type based policies i.e allow or deny, Bandwidth rate limit, VLAN mapping. The controller should also provide application visibility and control.	
32	The controller shall be manageable using CLI, Telnet/SSH, HTTP based GUI and SNMPv2/v3.	
33	The controller should be able to present a customizable dashboard with information on the status of the WLAN network.	
34	The controller should be able to raise critical alarms by sending an email. The email client on the controller should support SMTP outbound authentication and TLS encryption.	
35	The vendor should specify if all features are available with the basic access controller pricing or if the support of some features require the acquisition of some licenses. The vendor should specify which feature requires which type of licensing including its cost.	
36	Controller should have inbuilt BYOD features and Guest Access management procedure where user may use internet without entering to Enterprise SSID and should be time restricted. The Guest management should be a self-service one from end user perspective without the use of any additional software.	
37	The Controller should support WLAN that will allow users to login through social media like Facebook, LinkedIn, Google/Google+ or Windows Live.	

Krishna Sharma
 OFFICIATING PRINCIPAL
 P.G.D.A.V. COLLEGE
 Nehru Nagar, New Delhi-110055

	QoS features	
38	per SSID or dynamic Per user bandwidth Rate Limiting	
39	Self-healing (on detection of RF interference or loss of RF coverage) and vendor should provide their Interference mitigation techniques for same Domain interference (interference from AP's connected to same Controller) and from other AP's and 2.4Ghz devices (Microwave's, Radio's etc.)	
40	Dynamic RF management that provides the capability to pause channel scanning / adjust RF scanning intervals based on application and load presence.	
41	Capability to provide preferred access for "fast" clients over "slow" clients (11n vs. 11g) in order to improve overall network performance.	
42	System must support Band Steering where 5 Ghz clients are forced to connect over 5Ghz Radio to provide better load balancing among 2.4Ghz and 5Ghz Radios.	
43	Support advanced multicast features and WMM support to provide best performance on Video applications.	
44	Should have Voice Call Admission control	
	Client Management	
45	The controller should provide a Guest Login portal in order to authenticate users that are not part of the organization.	
46	The solution should be able to provide a web-based application that allows non-technical staff to create Guest accounts with validity for fixed duration like hours or days.	
47	System should be able to send password direct through Email and SMS to the user.	
48	System should be able to generate one click password for single user, multiple users or single user multiple devices.	
49	System should support internal and External Database for user authentication.	
50	System should support user management features like Rate limiting based on time based WLAN Access & User profile per WLAN etc.	
	Regulatory	
51	Wi-Fi Alliance certified	

Knishru

OFFICIATING PRINCIPAL
P.G.D.A.V. COLLEGE
Nehru Nagar, New Delhi-110065



1.5 Hardware controller managed 2*2:2 Indoor Wi-Fi 6 (802.11ax) Access Point

Specification / Requirement	Compliance (Yes/No)
The APs should support the IEEE 802/11a/b/g/n/ac/ax with dual radio capabilities conforming to Wi-Fi 6 standard.	
The AP should support 2x2:2 MIMO on both the bands. It should support minimum 1200 Mbps data rates on 5 GHz and minimum 574 Mbps data rates on 2.4GHz.	
The AP shall have two 1Gbps Ethernet port. Additionally, it should have an USB port for hosting Internet-of-Things (IoT) devices such as Bluetooth Low Energy (BLE) smart beacons. It should have integrated BLE and Zigbee 1 radio, switchable	
The access points should manage as standalone, controller and Cloud based.	
The access point should be able to operate in full MIMO mode and the necessary power POE/POE+ should be provided.	
Security mechanisms should be in place to protect the communication between the Access Point controller and the Access Points.	
The AP should have an option to be powered up through DC power in addition to POE.	
The AP should have a receive sensitivity of -96dBm.	
The AP should provide an antenna gain of minimum 3dBi on both the bands.	
The AP should support 20, 40, 80 MHz channelization.	
The access point should be able to detect clients that have dual band capability and automatically steer those clients to use the 5GHz band instead of the 2.4GHz band.	
The AP should provide minimum Tx Power of 22dBm on both the bands	
The access point should support 802.1q VLAN tagging	
The access point should support WPA-PSK, WPA-TKIP, WPA2 AES, WPA3, 802.11i security.	

Krishna sharma
 OFFICIATING PRINCIPAL
 P.G.D.A.V. COLLEGE
 Nehru Nagar, New Delhi-110065

The Access Point should provide for concurrent support for high definition IP Video, Voice and Data application without needing any configuration change. This feature should be demonstrable.	
The Access Point should support WMM, Power Save, Tx Beamforming, LDPC, STBC, 802.11r/k/v.	
The AP should have the capability to support minimum 15 BSSID	
Should support 500 or more clients per AP.	
Should support IPv6 dual stack from day one	
The Access Point should support mesh configuration either directly or through the controller.	
The Access Point should support rate limiting, application recognition and control, Access Control lists and device fingerprinting.	
Operating Temperature: 0°C to 50°C. Operating Humidity: up to 95% non-condensing.	
Should be plenum rated and comply to RoHS	
Should be WI-FI certified and WPC approved.	
Mechanism for physical device locking using padlock /Kensington lock / equivalent	

1.6 Hardware controller managed Indoor Wi-Fi 6 (802.11ax) 4x4:4 Wi-Fi Access Point with 2.5Gbps backhaul.

Specification / Requirement	Compliance (Yes/No)
The APs should support the IEEE 802/11a/b/g/n/ac/ax with dual radio capabilities conforming to Wi-Fi 6 standard.	
The AP should support 4x4:4 MIMO on 5 GHz and 2x2:2 on 2.4 GHz bands. It should support minimum 2400 Mbps data rates on 5 GHz and minimum 570 Mbps data rates on 2.4GHz.	
The AP shall have One 2.5Gbps Ethernet port and one 1Gbps Ethernet port. Additionally it should have an USB port for hosting Internet-of-Things (IoT) devices such as Bluetooth Low Energy (BLE) smart beacons.	

Krishna Sharma
 OFFICIATING PRINCIPAL
 P.G.D.A.V. COLLEGE
 Nehru Nagar, New Delhi-110065

The access points should be centrally managed as well capacity to work as standalone.	
The access point should be able to operate in full MIMO mode and the necessary power POE/POE+ should be provided.	
Security mechanisms should be in place to protect the communication between the Access Point controller and the Access Points.	
The AP should have an option to be powered up through DC power in addition to POE.	
The AP should have a receive sensitivity of -96dBm.	
The AP should provide an antenna gain of minimum 3dBi on both the bands.	
The AP should support 20, 40, 80, 160/80+80MHz channelization.	
The access point should be able to detect clients that have dual band capability and automatically steer those client to use the 5GHz band instead of the 2.4GHz band.	
The AP should provide minimum Tx Power of 23dBm on both the bands	
The access point should support 802.1q VLAN tagging	
The access point should support WPA-PSK, WPA-TKIP, WPA2 AES, WPA3, 802.11i security.	
The Access Point should provide for concurrent support for high definition IP Video, Voice and Data application without needing any configuration change. This feature should be demonstrable.	
The Access Point should support WMM, Power Save, Tx Beamforming, LDPC, STBC, 802.11r/k/v.	
Should support 500 or more clients per AP.	
Should support IPv6 dual stack from day one	
The Access Point should support mesh configuration either directly or through the controller.	
The Access Point should support rate limiting, application recognition and control, Access Control lists and device fingerprinting.	
Operating Temperature: 0°C (32°F) - 50°C (122°F). Operating Humidity: up to 95% non-condensing.	
Should be plenum rated and comply to RoHS	
Should be WiFi certified and WPC approved.	
Mechanism for physical device locking using padlock /Kensington lock / equivalent	

Krishna Sharma
 OFFICIATING PRINCIPAL
 P.G.D.A.V. COLLEGE
 Nehru Nagar, New Delhi-110055

[Signature]

1.7 Firewall Specifications:

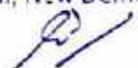
S. No.	Item	Specification of Next-Gen Firewall / UTM	Compliance to RFP specification whether Yes/No
1	Interfaces	<ul style="list-style-type: none"> ·Copper GbE port- 06 ~ 08 , with Flexi Port Option ·SFP Port ·Configurable LAN /DMZ/WAN ports ·Console Ports(Rj45)-1 ·USB port-2 ~4 ·VGA Port -1 	
2	Hardware Specifications/ Architecture	<ul style="list-style-type: none"> ·Rack Mountable on 1U Platform ·The proposed solution shall be of appliance based. ·Proposed appliance should have firmware residing on Solid State Drive (SSD) ·System Memory : 8GB ~ 16GB or better ·USB connectivity - minimum of 2 port ·VGA Console Port Support . ·The proposed solution should match the following criteria. <ul style="list-style-type: none"> a. Multi-Threads Architecture. b. Hardware platform must be 64 bit. 	

Krishna Sharma
OFFICIATING PRINCIPAL
P.G.D.A.V. COLLEGE
 Nehru Nagar, New Delhi-110065

li

		<p>c. Ethernet connectivity (Copper GbE) - Minimum of 6 ~ 8</p> <p>d. Proposed solution should have option for SFP Port Support over Flexi Port Module.</p>	
3	<p>General Requirement</p>	<p>·The product should be Product of India .</p> <p>·The proposed solution should have Product with Perpetual License.</p> <p>·The Total Solution shall be on-premise and shall not have any requirement to connect to any third party network for functional purpose.</p> <p>·The proposed solution must have tool to manage (FW configuration, Upgradation, troubleshooting etc) and monitoring of application, session and user traffic .</p> <p>·The proposed solution must have On-appliance Logging and reporting Feature and should not required any Log reporting server additionally</p>	
4	<p>System Performance</p>	<p>·Firewall Throughput : 18 ~ 20.0 Gbps</p> <p>·New Sessions /Second : 1,00,000~ 1,50,000</p> <p>·Concurrent Session : 75,00,000~1,00,00,000</p> <p>·IPSec Throughput : 1000 Mbps ~1500 Mbps</p> <p>·Secure SSL Throughput : 1000 Mbps ~1500 Mbps</p> <p>·GW AV Throughput : 1000Mbps~ 2500 Mbps</p> <p>·IPS Throughput : 1000 Mbps~ 3000 Mbps</p> <p>·UTM /USG Throughput : 2500 Mbps ~5000 Mbps</p> <p>·Storage (SSD) : 30 GB ~ 250 GB</p>	

Krishna Sharma
OFFICIATING PRINCIPAL
P.G.D.A.V. COLLEGE
Nehru Nagar, New Delhi-110065



5	Firewall & NAT	<ul style="list-style-type: none"> ·Stateful Packet Firewall ·Multiple security Zones ·Security polices-IPS, Web filtering , Application Filtering ,Anti-virus /Anti-Spam ·Access scheduling ·NAT: Network address Translation ·Policy based NAT (Source and destination) ·Gateway specific NAT policy ·Port Forward and Intercept Support ·One-to-one NAT ·SNAT ·Mac and IP-Mac Filtering ·IP- MAC Interface Binding ·Geo-IP Filtering: Geo Location based traffic control . ·Connection Per Second and time based firewall Rules 	
6	Networking & Routing	<ul style="list-style-type: none"> •WRR based Multi Load Balancing ·Automated failover / Fallback, ·Inbound Link Load balancing (ILLB) / DNS-based inbound load balancing ·IP address assignment- Static, Dynamic & PPPoE , ·Policy-Based Routing (Based on Zone ,Interface, IP/ MAC Address, Protocol or Port). ·Static Routes ·Source / Destination-Based Routing ·BGP routing Support 	

Krishna Sharma
OFFICIATING PRINCIPAL
P.G.D.A.V. COLLEGE
Nehru Nagar, New Delhi-110065

KS

		<ul style="list-style-type: none"> ·Proxy ARP ·Multiple DHCP server support (Should have Black List ,white List and Known Mac option). ·Supports HTTP/s Web Proxy (Traditional and Transparent Mode) . ·Dynamic Routing: RIP v1&v2 OSPF ,BGP . ·Multicast forwarding (Include Over SSL VPN). ·IP Pass-through Support. ·Reverse Proxy /WAF. ·Ethernet LAG (Link Aggregation Group) 	
7	IDPS (Intrusion Detection & prevention System)	<ul style="list-style-type: none"> ·Signatures: Default (2000+), Custom signatures / Polices ·Automatic real-time updates & e-mail notification and Offline Mode Update Option ·Traffic / Protocol anomaly detection and protection ·IPS actions: Recommended, Allow Packet, Drop Packet, Disable ·Flooding detection and protection 	
8	Web & Application Filtering	<ul style="list-style-type: none"> ·The Proposed Solution should Support Transparent and Non- Transparent Mode Web Proxy . ·The proposed solution must work as standalone HTTP proxy server with integrated . ·Web Authentication & inbuilt Web category Database support . ·Control based on URL/Content , Keyword . ·Control Based on Mime and File Extension Type : For both upload /Download Traffic . ·Protocols supported: HTTP,HTTPS. 	

Krishna Sharma
OFFICIATING PRINCIPAL
P.G.D.A.V. COLLEGE
 Nehru Nagar, New Delhi-110065

[Signature]

- The proposed solution should have a local database integrated into the system to avoid frequently querying a database hosted elsewhere.
- The proposed solution should have option to make Own custom database as per their need.
- Time-Based Access Control with Multiple Time Intervals
- Unlimited Policies & User creation
- CIPA compliant, Pornographic image blocking .
- Google Safe search enforcement & Restricted Youtube for Users
- Web Blocking Database Update (Both Online and Offline Mode)
- Should support custom database web category upload option
- HTTPS/SSL Interception Support
- Content Filtering based on Weighted Phrase
- The proposed solution must be capable of blocking the following types of applications.
 - a.Application that allow file transfer.
 - b.Online Games.
 - c.Instant messengers
 - d.Peer-peer(P2P) applications ,Tor and Torch Browser.
 - e.Browser Based proxy (regardless of Ip address or port Number).
 - f.Web2.0 based applications (Facebook etc).
 - g.Application that provide Remote control.
 - h.All type of streaming media (Both Web and Software Based).
- Group-Based and User-Based Web Content Filter

9

Mail Security &

Krishna Sharma
 OFFICIATING PRINCIPAL
 P.G.D.A.V. COLLEGE
 Nehru Nagar, New Delhi-110065



	Gateway Anti-spam	<ul style="list-style-type: none"> ·SMTP/POP3 mail intercept ·Image-spam filtering & Spam tag support ·Filter based on message header, size, sender, recipient etc. ·Blacklist / White list support ·Spam Tag support 	
10	Anti-virus and anti-malware	<ul style="list-style-type: none"> ·Real time checking or scanning at Gateway ·Ability to Scan while downloading ·Ability to Scan archive files ·Should not have size limitation on files for scanning ·AV signature Update (Both Online and Offline Mode) 	
11	Anti-spam & E-mail Security	<ul style="list-style-type: none"> ·Simple configuration and management •Content based anti-spam •RBL based anti-spam •Trusted domains/users list 	
12	Traffic Management / Quality of service (QoS)	<ul style="list-style-type: none"> ·Bandwidth Management and Throttling ·Guaranteed Bandwidth Based on rule Set ·Ingress traffic policing ·Priority- bandwidth utilization (User / Application) ·Preset File Sharing rules. ·Classified and Unclassified Bandwidth support ·Policy For Known and Unknown Ports 	

Krishna Sharma
 OFFICIATING PRINCIPAL
 P.G.D.A.V. COLLEGE
 Nehru Nagar, New Delhi-110055

(Signature)

13	High Availability (HA)	<ul style="list-style-type: none"> ·Hot Standby Active-Passive mode ·Support HA on WAN, LAN & DMZ ·Device failure detection and notification ·Heart Beat & Preempt mode support ·Link monitoring ·Auto-Sync configurations ·Device /Interface Failure Detection & Alerts ·Support both Member of Tracker & IP Migration ·IP Migration designed for Wireless networks as well ·Auto Sync Configuration. 	
14	Network Monitoring and Management	<ul style="list-style-type: none"> ·Comprehensive network monitoring; Logging record should at least contain Source IP, Destination IP, Type of Service, Timestamp, Type of Protocol, Port information etc... ·Customized flow ·Device failure Detection ·Actions: log/alert/SMS/reporting/logging ·Web based access ·Should support efficient searching and filtering to locate specific events in log record ·Should support bandwidth management per user, group, IP address, website Category, application & application category wise ·Link Failure Detection 	
15	VPN (Virtual Private		

Krishna Sharma
OFFICIATING PRINCIPAL
P.G.D.A.V. COLLEGE
Nehru Nagar, New Delhi-110065

[Signature]

Network)

I-IPSec VPN:-

- Support for Automatic and static IP
- Remote ID and Local ID Support
- Dead Peer detection (DPD) , IPSec NAT traversal & PFS support
- VPN Failover/ Connection redundancy & auto reconnect
- Interop with other IPSec devices
- FQDN support for tunnel end point /Remote WAN,
- VPN connection redundancy,
- Encryption Support- 3DES/DES /AES
- Authentication Support – SHA1 /MD5
- Support Key Exchange -IKE, Manual Key, PKI

II-SSL VPN :-

- True SSL/TLS VPN
- Encryption: 3DES, AES etc.
- Key Management & Certification authority.
- TCP & UDP tunneling.
- SSL VPN must support Site-to- Site and Client-to – Site VPN tunneling .
- Both server and client ends works with Dynamic Public IP
- Granular access control based on IP, Port & Time .
- Connection tracking based failover to SSL VPN over Captive MPLS VPN .
- Ability to Forcefully disconnect selected SSL VPN Clients.
- Bi -directional communication channel for data and voice over SSL VPN .

Krishna Sharma
OFFICIATING PRINCIPAL
P.G.D.A.V. COLLEGE
Nehru Nagar, New Delhi-110065

[Handwritten signature]

·VPN client support for Windows, Linux , Android & Mac OS.

·Auto VPN Failover / failsafe / VPN redundancy support.

·Network access- Split and Full Tunnel Mode.

·Hub and Spoke support.

·QoS support for SSL VPN Tunnel

·Support for VPN over HTTPS Proxy

·Multiple Server Support Scalability

·Support to the most advanced and standard cipher algorithms

Encryption: 3DES 192, AES 128/256-bit, SHA1/256/384/512

Authentication: Pre-Shared Key, Certification Authority, SMS OTP* , Googel Auth , MAC Address

& Local

III-PPTP VPN

·PPTP VPN with unlimited Tunnel License

·Forcefully Client disconnection Option

IV- WIRED GUARD VPN

·Must support Site-to- Site and Client-to – Site VPN tunneling

V-Other VPN Support

·Cisco VPN

·GRE Tunnel

Krishna Shrivastava
OFFICIATING PRINCIPAL
P.G.D.A.V. COLLEGE
Nehru Nagar, New Delhi-110065

K/S

16	Wireless WAN (W-WAN)	<ul style="list-style-type: none"> ·3G/4G USB Dongles with USB Tethering support . ·Primary WAN Link ·WAN Backup Link 	
17	HOTSPOT /BYOD (User Management)	<ul style="list-style-type: none"> ·Proposed Solution Should have Inbuilt AAA (Authentication, Authorization and Accounting) System. ·Should have Captive Portal Support . ·Customisable Users Login Page . ·Support both Wired Wireless Network. ·Manageable Internet access Usage Plan. ·Captive portal support based on IP address or IP Segment (multiple Captive portal support based on IP or IP Segments) ·Support to redirect the URL as per user requirement (Original request URL / Welcome Page / specific URL) ·Should Support User Management options Like - Create Activate Suspend Archive Users. ·Should Support On Appliance User Database with option to upload database in .xls format. ·Should Support Customized Packages options like : Define internet access plan based on Bandwidth ,Time & Data Quota. ·Product should support below QoS methods <ul style="list-style-type: none"> a. Bandwidth Management b. Bandwidth Priority c. Guaranteed Bandwidth d. Dynamic Bandwidth Control (automatically adjust the bandwidth based on users) e. No Ideal bandwidth waste ·Should have Bandwidth management with : Committed [Individual] Shared Bandwidth with Scheduling & Fair Usage Policy 	

Krishna Sharma
OFFICIATING PRINCIPAL
P.G.D.A.V. COLLEGE
Nehru Nagar, New Delhi-110055

K/S

·Should have **Coupon Management** with - Instant coupon generation in printable formats & System generated

·Should have **Packages management** with ; Self registration |OTP | Social Login |Pre-Paid & Post Paid

·Should have Per-User and Global Bandwidth Limiting.

·Group Management support per department wise with dedicated bandwidth allocation & separate admin panel to manage created users.

·Should have option of Time Based (Office | Non-office Hours) Bandwidth (min and max) for a particular User | MAC | IP.

·Device Blocking Support like Mobile / Tablet / Gaming console (BYOD) blocking during specified hours (HoS)

·To support check for MAC binding and MAC based authentication only for BYOD and allow the same user to login via standard browser login from Office network

·IP Segment based login restrictions for selected user Ids (means user A is allowed to authorize only from few configured IP segments)

·Device Blocking Support like Mobile / Tablet / Gaming console (BYOD) blocking during specified hours (HoS)

·Able to Auto-bind MAC address of 5 devices per user on BYOD level

·MAC-Address Based User Accounts .

·Auto Login Support based On MAC/IP.

·Auto MAC/IP Binding Support.

·User Accounts Upload / Import/Export via CSV .


·Automatic Client Network Configuration .

Krishna Sharma

OFFICIATING PRINCIPAL
P.G.D.A.V. COLLEGE
Nehru Nagar, New Delhi-110065

- Pre / Post-Paid and Free Tickets .
- Time / Traffic Based Tickets .
- Configurable Ticket Validity .
- Terms Login Support.
- Fair Usage Policy(FUP).
- Cyclic/Recurring Tickets (Daily | Weekly | Monthly | Yearly) .
- Time Quota(Daily | weekly |Monthly | Total | Lifetime).
- Data Quota(Daily | weekly | monthly | Total |Lifetime).
- Black List Management Support based On MAC| IP.
- Should support Self Registration Portal with options like
 - a.Create Mobile Account based on OTP
 - b.User Account creation with IT admin approval process
 - c.Prepaid Coupon with OTP Registration
 - d.Account Recharge on demand
- Remember User after First Authentication .
- Authentication Server Support (Local, LDAP/AD).
- Should Support option to Disconnect / Suspend 'Logged In' User for Particular time Period .
- This system should support integration more than 3+ SMS Gateways with Click-n-Configure.
- Should support Auto login blacklist of infected machine user(s)
- Should Support On-Appliance Connection Logging , Logs and reports


18	System Management	<ul style="list-style-type: none"> ·Three levels of users creation with preset permissions ·Multiple users login Option ·Web UI (HTTP, HTTPS & VGA) ·Command line interface (Console) 	
----	--------------------------	---	--

Krishna Sharma
 OFFICIATING PRINCIPAL
 P.G.D.A.V. COLLEGE
 Nehru Nagar, New Delhi-110065



		<ul style="list-style-type: none"> ·Configuration Backup & Rollback ·Firmware upgrade via web GUI ·Manual upload of Anti Virus Signatures IDS& IPS Signatures Web Blocking Database (Both Online and Offline Mode) 	
<p>19</p>	<p>Logging / Monitoring /Reporting/ Alert</p>	<ul style="list-style-type: none"> ·Comprehensive Local logging / Should have Inbuilt-on Appliance Reporting. ·Email Alert-Multiple Mail ID ·Built-in daily Digest report / Daily digest reports on email ·Remote Sys log support ·Real-Time traffic monitoring (Source IP /Port) ·Should have Built-in Network Tool – like TCP Dump, Live Network Sniffer etc . ·Should comes with all debugging tool inbuilt with live network real time net flow on IP and Port basis ·Should support Live Sniffer with users level Packet Per Second (PPS) to identify virus infected machines ·Should have option of Security Reports for Suspicious Activities. ·Graphical real-time and historical Monitoring ·Log Viewer- different kinds of logs including System boot long, firewall log, IDS/IPS, VPN, Web Proxy logs, Antivirus , Anti-spam, HA log, System and Admin events, IM activities Log etc ·Remote Management. 	

Krishne Sharma
OFFICIATING PRINCIPAL
P.G.D.A.V. COLLEGE
 Nehru Nagar, New Delhi-110065

	<ul style="list-style-type: none"> ·Alerts on Interface status Appliance reboot status Power status High Availability transition etc. ·Real Time Net flow on Individual interface wise data, which ensure the Top user based on Bandwidth Utilization Packet Per Second Usage per TCP /UDP Ports Applications . ·Should support Forensic analysis with quick identification of network attacks and other traffic anomalies. ·Should support complete Monitoring & Reporting Framework built in (NMS) at no extra cost (Detailed logs and Reports as per regulatory compliance) ·Should support mobile aware login pages and alert email / SMS on link failures 	
<p>20</p> <p>General configuration</p>	<ul style="list-style-type: none"> ·Software /Firmware upgrade using UI (Should Not mandatory Over Internet) ·The Proposed solution must have option to Upgrade Firmware /Patch/ Signature through Offline mode via Local Storage Media or Local LAN (Should not mandatory Over Internet) . ·Product Functionality (Like AV , Basic Web Filter and IDPS) should be work even if Non renewal of “Total security subscription suit” (Only its Update should be stop). ·Daily / weekly / Monthly backup on email and FTP (configurable option) ·All the configuration change logs should be provided in the Appliance ·Daily configuration backup archived by the product itself and can be downloaded on –will. ·Configuration snapshot on box itself 	

Krishna Shevme
 OFFICIATING PRINCIPAL
 P.G.D.A.V. COLLEGE
 Nehru Nagar, New Delhi-110005


		<ul style="list-style-type: none"> ·Data Quota Transfer per Interface wise with alert mechanism to admin ·System Security with HTTP / HTTPS / SSH access restriction to allowed IPs only ·User/IP/MAC binding functionality to map username & IP address & MAC address ·Show Configuration options to provide a printable record to the user on all the current running routing & Firewall configurations 	
21	Warranty & Support	<ul style="list-style-type: none"> ·Should provide all upgrades and/or patches free during Warranty period; ·Provisions for 4-year extended Subscription / warranty should be available after the 1 year Default Warranty / Total security subscription suit ·The OEM should provide Onsite technical support . ·The OEM should have regional presence. 	
22	On subscription Expiry.	<ul style="list-style-type: none"> ·Internet Security should continue to work . All the port should not be <u>Open</u> from Un-trusted (WAN) to Trusted network (LAN) or Vice-versa. ·Basic Web content filtering services should not be o <u>disable</u> web filtering protection due to subscription expiry and allow users to browse insecure & unsafe Internet. Only Update should be stop once subscription expired. ·Gateway Antivirus / Intrusion prevention should not be <u>disable</u> . GW scanning due to subscription expiry. Only Update should be stop once subscription expired. ·Basic HA should work even after Subscription Expiry. 	
23	Dimension	<ul style="list-style-type: none"> ·Not exceeding 1U; Rack Mountable 	

Krishna Sharma
 OFFICIATING PRINCIPAL
 P.G.D.A.V. COLLEGE
 Nehru Nagar, New Delhi-110065


24	Basic Training* On Firewall	To be provided by OEM -Onsite	
----	-----------------------------------	-------------------------------	--

General Requirements: (Technical Specifications)

- Brands under consideration includes but not limited to Ruckus, Cisco, HP, Juniper but must compliance all the technical specifications and All Wi-Fi components should be from single OEM.
- OEM should be in Wi-Fi domain for at least 10 years and should be present in India for minimum 8 years.
- OEM should have a development and support center in India
- Controller should support license for 40 AP's from day 1

Network Diagram/Layout Plan:

Before quoting the rates, the Contractors should inspect the PGDAV campus for understanding and estimation, nature & quantum of work. For visiting purpose our technical person Sh. Rajesh Khanna can be contacted at 9818182236 during office hours.

Scope of Work for Active and Passive networking at PGDAV College, New Delhi

A. Laying of Fiber Cable:

- Laying of Optical Fiber cable from Server Room to Old building (total 200m)
- Laying of Optical Fiber cable From server room to L shape new building (total 200m)
- Laying of Optical Fiber cable From Server Room to Canteen new building (total 200m)
- Laying of Optical Fiber cable From Server Room to Department block (total 200m)

B. Laying of cable as per below procedure:

- Laying of HDPE pipe and running of OFC cable through the pipe. Appropriate joints or couplings should be used whenever necessary.
- To run the cable along the wall or ceiling it can be done by running the cable in HDPE pipe. Wall/ceiling fixing hanger to be provided in each 1.5 meter distance.
- In some places, digging of soil or concrete of 2 feet (d) x 1 feet (w) about 100 meters
- Filling the digging area with cement concrete or soil wherever necessary.

C. Splicing of fiber cable:

- Fiber splicing and otdr testing of OFC at Computer hub
- Fiber splicing and otdr testing of OFC at Old Building
- Fiber splicing and otdr testing of OFC at L shape new building

Krishne Sharma
 OFFICIATING PRINCIPAL
 P.G.D.A.V. COLLEGE
 Nehru Nagar, New Delhi-110065

K/S

- Fiber splicing and otdr testing of OFC at Department block
- Proper ferrule details and cable marking tags to be provided.
- Splicing, cable marking, ferrule details to be recorded and shared with PGDAV staff.

D. Passive networking and related tasks:

- UTP Cable Laying through PVC Pipe on the wall or ceiling as required
- UTP cable laying in conduit from Computer / server room rack to designated AP locations
- UTP cable laying in conduit from new building rack to designated AP locations
- UTP cable laying in conduit from canteen building rack to designated AP locations
- UTP cable laying in conduit from department block rack to designated AP locations
- UTP cable laying in conduit from old building rack to designated AP locations
- UTP cable laying in conduit within certain racks to internetwork
- Installation of 6 network rack
- Labeling of Cables, I/Os, Jack Panel, Switches, firewall and WLAN equipment for new connections
- Patch cord should be branded and factory crimped.
- Equipment furnished shall be complete in every respect with all mountings, fittings, fixtures and standard accessories normally provided with such equipment's and/or needed for erection, completion and safe operation of the equipment's as required by applicable codes though they may not have been specifically detailed in the tender document, unless included in the list of exclusions. All similar standard components/parts of similar standard equipment's provided, shall be inter-changeable with one another.
- Creation of documentation to be shared with the college.

E. Active networking

- Installation and configuration, testing of WLAN controller in HA mode
- Installation and configuration, testing of WLAN AP in designated location and points to be provided optimum coverage
- Installation and configuration, testing of 8 and 12 port poe switch respective locations network racks
- Installation and configuration & testing of NGFW/UTM in computer room.
- Documentation of satisfactory test results to be provided to college.
- Integration of active components with current/existing active setup.
- Integration of WLAN controller and AP with AD/Radius for authentication.
- Bidder will responsible to mount, install and configure all switches as per required locations.
- Firmware software, license and required patched should be upgraded on the switch.
- Network configuration like VLAN and security config should be done as per our existing network.
- Warranty status for all active switches should show on OEM portal.
- Network Documentation of implemented setup should have submitted by bidder to the ICGEB.
- Creation of WLAN policies for Student and staff for QOS, security and usage.
- Setting up of alerts and alarms in all active components.
- Physical installation and powering of all Active and Passive components as per details provided.
- Train in-house engineers on wireless technologies, WLAN controller and AP solution.
- Validate the performance, quality, and reliability of the WLAN solution implemented..

F. Test Report:

- OFC Communication test to be done in front of PGDAV Staff only

Krishne Sharma
OFFICIATING PRINCIPAL
P.G.D.A.V. COLLEGE
Nehru Nagar, New Delhi-110015

[Signature]

General Terms and condition

- The intending Bidder, in case of Authorized Dealer shall possess valid authorized Distributorship / Dealership license from Prime Equipment manufacturers. The Bidder shall enclose the copy of the same and also provide **manufacturer authorization form** for this requirement while submitting the Bid.
- The documents consisting of inviting the Offer, Scope of work, General rules and instructions to the Bidder, Bid Opening and Evaluation, Technical specification and other annexures documents can be downloaded from the college website. Any clarifications / amendments / corrigenda etc., to this Bid Notice before last date of submission of bid will only be available on our website. Therefore, bidders are advised to keep visiting our website
- The bidder needs to submit bids in "TWO ENVELOPE CONCEPT" and it has to be submitted as such the first envelope should contain all the components of Technical Bid detailed with all supportive documents duly signed on all the pages. The envelope shall be sealed & super scribed as "**Technical Bid - Optical Fiber/WiFi Networking PGDAV College**". Bidder should note that financial aspects of the offer should not be disclosed in any way, in the technical bid/ first envelope and such technical bids consisting of financial aspects are liable for rejection.
- The second envelope should contain the financial Bid i.e. the Price Bid of Quantities and shall be super scribed as "**Financial Bid - Optical Fiber/WiFi Networking PGDAV College**" and should be sealed and submitted on the same given date and time simultaneously along with technical bid. Non submission of the same (Financial Bid) in separate sealed cover along with technical bid shall automatically render the entire offer being rejected. This envelope should contain duly filled in cost details (enclosed in the offer document).
- The Sealed Bids should reach PGDAV College, New Delhi on or before 21 days of publication of this tender document on college website.
- The Bid shall be completed in all respect and should be signed with date by the Authorized Signatory of Bidder with company stamp on all the pages of this Bid.
- While submitting the Bid, if any of the prescribed conditions are not fulfilled or are incomplete in any form, the Bid is liable to be rejected. If any Bidder stipulates any condition of his own, such conditional Bid is liable to be rejected.
- PGDAV College reserves the right to reject any Bid/ bid wholly or partly without assigning any reason.
- The Bidder shall be agreed that the rates submitted shall remain valid for acceptance for a period of 60 days from the date of opening of the Bid.
- Bidder shall take into account all costs including installation, commissioning, cartage etc. for giving delivery of material at site i.e. PGDAV College, New Delhi before quoting the rates. In this regard no claim for any extra payment for any reason shall be entertained.
- The material shall be inspected on receipt at site PGDAV College, New Delhi and bidder shall be responsible for any damage during the transit of goods.

Krishna Sharma
OFFICIATING PRINCIPAL
P.G.D.A.V. COLLEGE
Nehru Nagar, New Delhi-110005

- The Bidder shall be responsible for providing all materials, equipment's, and services, specified or otherwise, which are required to fulfill the intent of ensuring operability, maintainability, and reliability of the complete equipment covered under this specification within his quoted price.
- This work shall be in compliance with all applicable standards, statutory regulations and safety requirements in force of the date of award of this contract.
- The bidder shall also be responsible for deputing qualified personnel for installation, testing, commissioning and other services under his scope of work as per this specification. All required tools and tackles for completing the scope of work as per the specification is also the responsibility of the bidder. Quoted cost must cover all accessories like hardware, clamps, SFP modules, tape, tools, connectors, cable tie, Labels, transport/cartage.
- The bidder should ensure while installation of LAN, day-to-day functioning of official work and existing network setup/connectivity/internet connectivity should not get disrupted.
- The bidders proposal shall include the list of tools (such as crimping tool, Krone punch tool) and other accessories, which are required for installation of the connection. No separate charges for fixing/crimping/other connection charges would be paid by PGDAV College.
- Any structure, permanent or temporary, dismantled or destroyed during the execution of the work shall be refilled/remake or restore to its original condition by the contractor at his own cost.
- Any extra electrical points and data points required in the server room shall be provided by college
- The required UPS power points in the rack shall be provided by college.
- Configuration and Integration of all of Active and Passive components as per the agreed and approved implementation plan to be shared after award of work.

GENERAL TERMS AND CONDITIONS OF THE BID

Note: Bidders must read these conditions carefully and comply strictly while submitting their bids.

MINIMUM ELIGIBILITY CRITERIA for the bidder

The bidder should meet the following Eligibility Criteria and must submit documentary evidence in support of their claim for fulfilling the criteria and they should submit an undertaking on their official letterheads to the fairness of these documents while submitting the bid. The bids received without the documentary evidence will be rejected outright.

1. The Bidder, should submit the turnover per annum for the last three audited years (FY2016-17, 2017-18, 2018-19) in similar kind of business with documentary evidence.
2. Copies of the work order and completion certificate successfully executed for similar kind work during the last 7 years.
3. A) Bidder should have successfully completed one single assignment of similar kind for Rs.10,40,000/- B) Two similar work of Rs 6,50,000/- each and Three Similar work of Rs 5,20,000/-each.
4. The bidder should have valid GST/TIN, Service Tax, registration certificates from relevant authorities (provide latest receipts/challans for documentary evidence).

Krishna Sharma
OFFICIATING PRINCIPAL
P.G.D.A.V. COLLEGE
Nehru Nagar, New Delhi-110065

5. The bidder should submit PAN number with documentary evidence
6. All the bidders shall have to produce documentary evidence for the same.
7. The intending Bidder, in case of Authorized Dealer shall possess valid authorized Distributorship / Dealership license from Prime Equipment manufacturers. The Bidder shall enclose the copy of the same and also provide **manufacturer authorization form** for this requirement while submitting the Bid.
8. Bidder shall be ISO-9001 certified firm

PREPARATION AND SUBMISSION OF THE BID DOCUMENT

Technical Bid (One fully sealed Envelope containing flowing details and marked as Technical Bid - Optical Fiber/WiFi Networking PGDAV College)

Name of the Contractor (Firm / Individual) and contact person:

Date of incorporation of the Firm:

Address of the Registered Office:

Telephone No./Mobile No.:

Fax No./E-mail ID:

Whether proprietary / partnership:

PAN No. of the Proprietor / Company:

Name & Address of the partner, if any

Total turn-over of the firm during the last 3 years

Work orders and completion certificate of completed one single assignment of similar kind for Rs. 10,40,000/- or Two similar work of Rs 6,50,000/- each or Three Similar work of Rs 5,20,000/-each within the previous 7 years.

GST/TIN No. & Service Tax Registration No:

Enclosures:

- Certificate of registration (GST PAN).
- Documentary evidence for minimum qualifying criteria.
- Turnover certificates of last 3 years
- Undertakings / declaration certificates
- Tender Document of technical compliance as per format mentioned under 'Technical specification of Active Component' above (duly signed on all pages).

Financial Bid (One fully sealed envelop marked as Financial Bid - Optical Fiber/WiFi Networking PGDAV College)

- Price Bid (Schedule of Rates) as per format mentioned under 'Items required' above.

The cost break-up should be clearly detailed and GST / sales/ service and other taxes as applicable should be shown separately. At the bottom please mention the total of each Active, Passive and Service Component and finally a grand total.

Rishna Sharma
OFFICIATING PRINCIPAL
P.G.D.A.V. COLLEGE
Nehru Nagar, New Delhi-110065

[Signature]

Payment Terms and Completion Time

- (a) 10% mobilization advance of work order value against bank guarantee of equivalent amount.
- (b) Additional 50% of the work order value against supply all active & passive items with accessories.
- (c) Balance final payment after completion of the work and submission of the final bill.

Time limit for completion of the work is 60 days from the date of the order issued. The time shall be the essence of this contract and entire work as titled above is to be completed in all respects within the given time from the date of issue of work order. The successful bidder has to submit the time & activity chart for the completion of work.

Termination of Contract

The Principal, PGDAV College, reserves the right to terminate the contract on account of poor workmanship, failure to mobilise the site within 30 days, non-compliance of set norms/specifications for the works, delay in progress of work etc.

Kishu Sharma
OFFICIATING PRINCIPAL
P.G.D.A.V. COLLEGE
Nehru Nagar, New Delhi-110065

Kishu