TECHNICAL SPECIFICATIONS FOR EXTRA LOW VOLTAGE (ELV) WORKS

TABLE OF CONTENTS

I. PREFACE

A. Tropical Conditions

All equipment/material supplied against respective Specification shall be suitable for satisfactory continuous operation, storage & maintenance under tropical conditions as specified below:

- Ambient temperature : 45 degree Celsius
- Annual Average Relative humidity : 50%
- Isokeraunic level (days per year) : 50
- Seismic Zone : Zone-IV
- Climate type : Moderately hot and humid tropical, climate, conducive to rust and fungus growth

B. General:

The Security work shall be carried out in accordance with Indian Standard Code of Practice. It shall also be in conformity with the current Indian Electricity rules and regulations and requirements of the Local Electricity Supply authority and Fire Insurance regulations so far as these become applicable to the installation.

The scope includes the jobs to be performed for all equipment and materials furnished under this specification. The scope is however not limited to the items detailed below:

- Design, manufacture, testing at manufacturers works packing and dispatch.
- Transportation to site and insurance.
- Receiving at site, unloading, handling, opening, inspecting, reporting and submitting claims in case of damages and short supply items.
- Arranging to repair/re-ordering all damaged and short supply items.

II. SPECIFICATION

A. Intelligent and Addressable Fire Detection & Alarm System

1. Scope

- This specification outlines the requirements for an intelligent, addressable fire detection and alarm system.

- The work described in this specification consists of all labour, materials, equipment and services necessary and required to complete, test and commission the fire detection and alarm system. Any material not specifically mentioned in this specification or not shown on drawings but required for proper performance and operation shall be provided and installed for a complete and operational system, by the contractor at no extra cost.

- The contractor shall furnish, and install complete and ready for intended use and operation, an intelligent, addressable fire detection and alarm system including Fire panel (s), initiating devices (manual pull stations, addressable smoke, heat detectors etc.) indicating devices (hooters, bells, visual warning signals, etc.) and supervisory devices, annunciators, wiring apparatus and accessories.

- The installation and locations of equipment and devices in the building shall be governed by the specifications and drawings with due regard to actual site conditions, manufacturers' recommendations, ambient factors affecting the equipment and other operations in the vicinity. If any departure from the specifications or drawings is necessary, approval shall be obtained from the Engineer-in-Charge before work is started thereon.
- Materials and equipment shall be new, first grade, standard, current models of the manufacturer and shall be suitable for this system. Where two or more pieces of equipment performing the same function are required, they shall be exact duplicates produced by the same manufacturer.

- All materials, devices, and equipment shall be compatible with the circuits or systems in which they are utilized.

- The Contractor shall submit specific catalogue cuts for each of the item specified in BOQ for approval from Engineer in charge before procurement.

2. Definitions

- **Alarm Indicating Circuits**

  Circuits to which alarm indicating devices are connected. Alarm indicating devices are audible or visual devices for warning building occupants. They include but are not limited to alarm bells, hooters and visual warning signal lights.

- **Alarm Initiating Circuits**

  Circuits to which automatic or manual alarm initiating devices are connected. Alarm initiating devices include manual pull stations, addressable fire (smoke) detectors, beam detectors and other emergency reporting devices.

- **Alarm Signal**

  A signal which signifies a state of emergency requiring immediate notification of the fire services.

- **Smoke, Heat Detectors**

  A detector which detects heat or smoke and is Analog Addressable type with switches/codes etc. to define the Detector.

- **Manual Call Point**

  A device which shall be addressable type with switches/codes etc. to define the station. Function shall be similar to that of a conventional Manual Call Box.

- **Hooter**

  A device which shall be able to give audible alarm through it and controlled from the Fire Alarm Panel. It can also be used for Public Address during emergency situation.

- **Fault Isolator**

  This equipment shall be placed in the electrical wiring and shall be able to isolate electrical short circuiting and loose wiring. The isolator shall be able to keep the part of the electrical circuit in operation that is connected directly to the Fire Alarm Panel.

- **Fire Alarm Panel**

  This refers to the microprocessor based Panel that shall be connected to the various Detector loops. There shall be multiple looping/zoning as indicated on the drawing. The panel shall be able to watch individual Detectors for performance as well as to give pin point location of fire alarm. Hooter Alarm as well as facility for cutting off of A.H.Us and electrical power is also included in this panel.

- **Loop**

  A loop or a zone shall mean a 2 wire circuit connecting at least 240 detectors and devices in any combination

- **Control Modules**

  These shall on getting the signal from the Fire Alarm Panel shall trip AHUs power supply etc. as required.

3. Requirements

This installation shall be made in accordance with the drawings, specification, local codes and local fire authorities having jurisdiction over this project.

4. Reference Standards

The design, supply, installation, testing and commissioning of the entire fire detection and alarm system shall conform to BS:5839 or NFPA 71 and 72. The Detectors shall conform to relevant codes for Fire Alarm System.

The system installed shall comply with the following codes/publications:

- IS 2175
- IS 2189
- IS 11360
- IS 732
- UL "UNDERWRITERS" laboratory/NFPA/FM/VDS/FOC for addressable detector, fire panel.
- EN 54
- BS 5445

5. Tests at Site

All commissioning tests at site will be in line with BS : 5839 or NFPA 71 and 72. Following test shall be conducted

- Loop Checking
- Checking of smoke detectors, Heat detectors etc. by simulation.
- Functional tests for fire alarm panel.
- The Mock trial of the complete Fire Detection and Alarm system.

6. Tests at Manufacturer's Work

- Tests certificates will be furnished for approval of all Fire alarm devices and system devices.
- All routine tests as per relevant codes for the Fire Alarm Panel, shall be conducted and results furnished to the Engineer-in-Charge.

7. Shop Drawings

Shop drawings submitted by the Contractor shall contain the following:

- Block Diagram showing all detectors and devices area wise, their connectivity to the panel including wire description.

- Point-to-point wiring diagrams showing the points of connection and terminals used for all electrical field connections in each system, all equipment or systems which are supervised and controlled by the fire alarm system. Diagrams shall show all connections from field devices to the control panel initiating modules, output modules, switches, relays and terminals. Diagrams shall show interconnection of all devices, modules, output

modules, switches, relays and terminals.

- Custom Build software for project with loop/device annunciation description and automatic control functions for each specific loop/device.

8. Power Supply

- The control panel shall derive 230 Volts power from main supply. A standby power supply shall be immediately available in the event of failure of normal supply and shall automatically be connected so as to maintain the equipment in condition such that fire alarm originating from the operation of Detector can be given. The standby battery as secondary supply shall be such that when charged by associated battery charging equipment it can operate independently for a period of 12 hours. It shall have enough power supply to cope with additional load resulting in alarm originated from two separate zones for the one hour. Batteries shall be of Lead Acid type and sealed Maintenance free.

- Suitable arrangements shall be incorporated to prevent secondary batteries from discharging through the charging equipment in the event of its breakdown or a failure in the supply.

- In addition to the batteries, a battery charger suitable for operation on the auxiliary power available in the plant as specified above shall be supplied. The capacity of the charge shall be such that the same can boost charge the battery (within 8 hrs) while supplying the rated load of the fire detection and annunciation system. Facilities shall be provided to limit the voltage supplied to fire detection and alarm system to their rated values during the time of boost charging. The charger shall normally supply the battery trickle charging current and the DC load of the fire detection and alarm system. In case the AC supply on the input side of the charger fails the necessary power for the complete fire detection and alarm system shall be supplied by the battery.

- Visible and audible annunciation for troubles or failure in the power supply system like "charger Failure", "Battery Low Voltage", etc. shall be provided.

- Battery earth/fault indication/annunciation shall be included in the panel.

9. FIRE ALARM SYSTEM DEVICES

- **General**

  Each device shall be assigned a unique address via easily understood decade (01 to 99) switch. Address selection via binary switches or by jumpers is not acceptable. Devices which take their address from their position in the circuit are unacceptable because if devices are later added, existing addresses, descriptors and commands need to be reprogrammed.

  Devices shall receive power and communication from the same pair of conductors. For fault isolating modules a separate power wiring which shall be fault tolerant shall be provided.

  Each device shall contain screw terminals with rising plates for positive termination suitable for 1.5 sq.mm. copper conductor wire.

- **Addressable Manual Stations**

  Manual stations shall be of rugged die cast construction designed for semi-flush mounting. Plastic stations will not be acceptable. Stations shall be of the break-glass design and must be opened to be reset. Closing the box after opening it shall automatically perform the reset function. It shall be possible, for testing purposes, to initiate an alarm without breaking the glass. All stations shall be furnished with a spare glass break rod.

Provisions shall be made such that the address cannot be changed merely from opening the station.

- **Addressable Analog Detectors**

All fire sensors shall mount on a common base to facilitate the changing of sensor type if building conditions change. **The base shall be incompatible with conventional detectors to preclude the mounting of a non-intelligent device.**

If the Fire Alarm Panel determines that the sensor is in alarm, the Fire Alarm Panel shall command the sensor LED to remain on to indicate alarm.

Each sensor shall be capable of being tested for alarm via command from the Fire Alarm Panel.

Each sensor shall respond to Fire panel scan for information with its type identification to preclude inadvertent substitution of another sensor type. The Fire Alarm panel shall operate with the installed type but shall initiate a mismatch (trouble) condition until the proper type is installed or the programmed sensor type changed.

Each sensor shall respond to Fire Alarm Panel scan for information with an analog representation of measured fire related phenomena (smoke density, particles of combustion, temperature). Such response proves end-to-end sensor including the operation of the sensor electronics. **Systems which only monitor the presence of a conventional detector in an addressable base shall not be acceptable.**

The Detector shall meet the requirements of either EN 54 or shall be listed with UL. It shall be possible to test the Detector's working both from the Panel as well as locally by means as designed by the Contractor and approved by the Engineer-in-Charge. The approved coverage per Detector for unhampered areas shall not be less than 50 sq. M. The detector shall be capable of being reset automatically after any alarm condition.

- **Addressable Analog Heat Detectors**

The Detector shall be Analog, Addressable Detector with its own manually set digital code and be able to give a single digitised output to the Fire Alarm Panel regarding its condition. The Detector shall employ the thermistor principle for heat sensing and the fixed temperature setting shall be at 60 degrees Centigrade. It shall be able to communicate with the Fire Alarm Panel by the Pulses emitted from the Panel.

The Base of the Detector shall be interchangeable with other Smoke Detectors and the construction shall be of flame retardant material. LEDs shall be provided to indicate locally alarm condition.

It shall be able to withstand temperature variations from 0o C to 50o C. Further, relative Humidity (non Condensing type) upto 95% shall not hamper its performance.

It shall have in built safety device to monitor the removal and pilferage of the Detector. The Detector also must have facility for remote indication. The quiescent current flow must not exceed 50 milli amps. and alarm condition current shall be maximum 60 milli amps.

- **Alarm Hooters**

Alarm hooters shall be suitable for indoor, or outdoor, application with the appropriate 4 x 4 in. electrical box. All hooters shall be 24 V DC operated. The minimum sound level shall be 90 db at 10 feet. Hooters shall be surface semi-flush mounted.

- **Monitor Module**

  The monitor module shall provide an addressable input for N.O. or N.C. contact devices such as manual stations, waterflow switches, sprinkler supervisory devices, etc.

  It shall provide a supervised initiating circuit. An open-circuit fault shall be annunciated at the Fire Alarm panel (Subsequent alarm shall be reported).

  The device shall contain an LED which blinks upon being scanned by the Fire Alarm panel. Upon determination of an alarm condition of an alarm condition, the LED shall be latched on.

- **Addressable Control Module**

  Addressable Control Module shall be provided to operate dry contacts for switching ON OFF Pressurisation fans, AHU' s etc. in case of fire etc. It shall have a built in type identification to automatically identify this device to the control panel. It shall have internal circuitry & relay powered directly by two-wire loop.

- **Fault Isolator Device**

  The Fault Isolator Device shall detect and isolate a short-circuited segment of a fault-tolerant loop. The device shall automatically determine a return to normal condition of the loop and restore the isolated segment. The fault isolator device shall be placed every [20] devices to limit the number lost in the event of a short-circuit.

10. Fire Alarm Panel

Fire Alarm panel shall be provided with 80 character backlit Liquid Crystal Display (LCD) Annunciator, function key pad, and printer as specified below. Necessary software and hardware shall be furnished at the location shown on the drawings.

- **Automatic Functions**

  The alarm shall be displayed at the FP on an LCD display. The FP printer shall print out the same information displayed on the LCD display.

- **Manual Functions**

  At any time, the operator shall have the following manual capabilities at the FP by means of switches located behind a key locked cover:

  - ❖ Initiate an alarm summary display on the FP LCD display. This display shall step through all currently active alarm in the system.
  - ❖ Initiate a summary printout of all currently active alarms on the FP printer.
  - ❖ Initiate an "all point summary" printout on the FP printer recording the status of each system point (initiating circuits, indicating circuits, etc.)

  At any time the operator shall have the following manual capabilities at the FP under password control.

Operator privileges and ID numbers of up to four digits shall be assignable only by the main operator or designated alternate. Actions taken by operators shall automatically be printed on the FP printer with operator initials, time and date.

- Command output points to different mode. Such commands shall be printed with selected descriptors ON/OFF, ON/OFF/AUTO, OPEN/CLOSE, DAY/NIGHT, etc.

- Modify system parameters. Full alphanumeric key pad shall be provided for operators to modify the following parameters:-

  - change sensor alarm and prealarm thresholds
  - update date and time
  - change point descriptions
  - change action messages

- Select a system status report for printing on the FP printer. The following real time reports shall be provided:-

  - all point log
  - alarm summary
  - trouble summary
  - status summary
  - sensitivity log
  - disabled points log
  - isolated points log
  - disconnected points log
  - logical group points log

  The sensitivity log shall print the analog value of each addressable analog sensor.

- Select printing of a trend log which, when enabled, shall print the last 24 analog values for every addressable analog sensor taken at predetermined intervals selected by operator. Systems which limit the number of addressable analog sensors which can be trended are not acceptable.

- Select a sequence of preprogrammed commands which shall be automatically executed, in sequence, via a single command. Provide a minimum of 255 commands which can be divide among a minimum of seven sequences.

- Perform a walk test function such that a single operator can periodically check out all initiating devices on a loop. In walk test mode all initiators on the selected loop shall automatically be isolated. As each device is placed into an alarm or trouble condition the FP shall print the condition and automatically reset the device. No audible signals shall be initiated from the loop to prevent disruption of building occupants. If a loop is inadvertently left in the walk test mode it shall automatically reset to normal after a five minute idle time is exceeded.

- **System Supervision**

  - In the normal supervisory condition, only the green "POWER" LED, and green "RUN" LED shall be illuminated. The LCD display shall display "System Normal" and the current time and date.

  - The LCD display shall indicate the loss of power condition and the printer shall record same. Following restoration to normal AC power, the trouble indicators shall be automatically reset, and the printer shall record the return to normal condition.

- ❖ The LCD display shall indicate the loop in trouble and the printer shall record same. Operation of a momentary "Silence" switch shall silence the audible trouble signal, but the visual "Trouble" LEDs shall remain on until the malfunction has been corrected and the system reset. The FP printer shall record this action.

The FP shall contain an integral backlit LCD display of two lines of 40 characters each, **and a 40 character width printer**. Both display and printer shall be viewable through the FP door.

- **Programming**

The LCD display and printer programming shall be accomplished on-site by means of a lap-top personal computer which shall plug into the FP. Modules requiring off-site programming are not acceptable. Programming functions shall include alarm/trouble type assignment, point descriptor assignment, etc. Data file for the LCD display and printer shall be stored in EEPROM.

- **Networking**

An additional output drive card must be provided to facilitate networking between two or more panels.

11. Approval of Fire Detection and Alarm System

The Contractor has to get the drawings for Fire Detection and Alarm System approved from the local fire authorities. On completion of the work, the Contractor has get the installation approved and obtain a certificate from the local fire authorities and handover the same to the Construction Manager. **The fees required for obtaining the approval shall be reimbursed by the Construction /manager on actuals, on submission of documentary proof.** The contractor shall be responsible for obtaining the required approval from Tariff advisory committee and other statutory authorities.

12. Testing & Commissioning

- **Photothermal Smoke and Heat Detector**

- ❖ The testing shall be carried out for each loop initially with one detector in a loop and subsequently two or more disassociated detectors in each loop with time gap between the detectors for alarm acknowledge and Reset.

- ❖ An identified smoke detector will be subjected to smoke aspiration from burning paper or cigarette puffs, held at 0.3 m distance from the detector. The panel should indicate through piezo sounder and hooter that alarm signal has been transmitted throughout the system. This test shall be carried out in different loops as well as two loops simultaneously. This part of the detector test shall be repeated again after 24 hours gap.

- ❖ The same test in the same sequence shall be carried out for heat detector but with the application of heat from a hair dryer-held at approximately 60 cm distance. Repeat testing of the same detector shall be carried out at 24 hours interval.

- **Combined Test**

- ❖ The panel shall be checked for basic tests, such as, visual checking of input voltage and amperage. All loops one by one, shall be D-wired to check for fault signal indication in the panel.

- ❖ Subsequently, in every loop of panel, a detector shall be subjected to smoke or heat test and signals shall be checked on the panel.

- ❖ The hooter shall sound automatically and the piezo sounders shall also sound. It shall also be possible to check that the hooters of all panels sound automatically when the panels are auto moded.

- ❖ The power source shall be cut off and checked for standby supply from the batteries. After six hours the power source shall be switched on to check for auto switch over to mains mode. The trickle charger shall take over the charging of the battery to its maximum cut off level with auto cut off. A set of discharged batteries shall be connected to the panel in place of the new batteries and the trickle/boost switch checked for charging of the batteries.

- ❖ Tests shall be conducted for AC failure, charger failure, battery disconnected or battery failure. In all such cases the relevant indication should come and the sounder shall also sound alarm.

- **Manual Call Box**

  The manual call box glass shall be removed by unscrewing the back. The micro switch shall instantaneously give a fire signal in the panel.

- **Random Sample Testing**

  About 5% of all fire alarm components shall be subjected to random testing by connecting to the panels. All smoke detectors shall be tested as given above and later cleaned with a vacuum cleaner. Hooters shall also be tested through direct 24V supply. It shall be tested for 10 minutes.

- **Testing of Earthing system**

  The earth continuity conductor including metallic parts of the equipment's shall be tested for earth to electrical continuity. All tests shall be carried out as per IS 3043 and resistance of complete installation shall not be more than one ohm.

- **Commissioning and Acceptance Tests**

  The commissioning and acceptance tests shall be apart from the standard or routine tests prescribed and normally conducted by the manufacturer and will be irrespective of the fact whether the same are covered by such tests or not.

  - ❖ Each sounder circuit shall be energized separately and the sound level reading taken to check for conformity with the minimum standards.
  - ❖ Mains failure performance.

  - ❖ Battery disconnection test.

  - ❖ Open circuit of each sounder circuit to be tested.

  - ❖ Short circuit of each sounder circuit to be tested.

  - ❖ The results of the above tests either by fault warning or fire alarm shall be recorded in the log books which will be signed both by the Consultant and Engineer in charge.

B. Access Control System

1. Scope

This section covers the Supply, Installation, testing and commissioning of Access Control System.

The Access Control System shall be provided so that the entry of persons shall be controlled by card reader. The exit of persons shall also be controlled by Card reader.

2. Access Controllers

The access control unit shall have the capacity to connect via coaxial cable proximity card reading sensors and contact inputs for alarm and status report. Controller shall provide operation of electrified locking hardware by means of (2) plug in dry contact fused relays each with a rating of 3 amps.

The Unit shall be designed to operate properly within relative humidity range of 10% - 95% non-condensing and within a temperature range of -7° C to 50° C.

The Unit shall be wall mounted and all wiring connections shall be provided at the top. Power should be available from a separate/built in power supply unit capable of providing power to the unit, sensors and other annunciator devices.

The controller unit should have 2 nos RS. 232 data I/O ports for encoded data and be capable of being connected directly to a printer.

The Unit shall contain a minimum database of 10,000 keys with unique number identification. It should store user operating data and handle alarm reporting for upto (2) card reading sensors and report activity for upto (8) monitored inputs. It should initiate relay outputs commands based on card access activity, operator keyboard inputs, preprogrammed time schedules and switch inputs. System diagnostics and automatic alarming based on detected faults in sensors, cables or devices connected should be inbuilt.

The unit should provide off line diagnostics for checking the integrity of the RAM And EPROM memory.

The Unit should be capable of being connected with auto dial up modems to automatically report or send messages to local/remote terminals and be capable of off site programming via dial up modems.

The access controller shall have the following features defined:

3. Access Codes

Access codes shall define when and where the card holder will be granted access. Each access code shall have the capability of defining upto four time periods for each entry point in the system. A time period shall indicate time of day, day of week and holidays.

4. Key commands

The user shall be able to define upto 10,000 keys with a unique numeric identification. The user may bulk programme keys in groups and remove any key from the database. Any key usage shall be traced by the system and a key trace report generated. Key functions shall include:

Access

The access parameters shall be defined such that any single key can be programmed to open each entry/exit point during four different time periods. System shall be capable of having upto 64 different time intervals. Key access parameters may be modified at any time.

Antipass back

The unit shall have the capability of designating any key/(s) so that when it is used to enter an area it must be used to exit that area before it can be reused for entry. The system shall have two modes for this operation:

- Hard: Denies entry and reports pass back violation.
- Soft: Allows reentry but reports pass back violation.

Alarm Shunting

System shall have means to connect presence detecting devices to shunt alarms when unauthorized exit takes place.

Forced Entry Alarms

The system shall report forced alarms.

Passwords

System shall be capable of identifying eight different operators for terminal use. up to 12 character user definable passwords shall used to log onto the system. Up to 6 access levels having different function capabilities shall available.

Printed Data Output

The unit shall be capable of printing the following information without any external computer interface:

- Key codes, Names, Access Codes, Location, Key Trace Function.
- Monitored Point Parameters.
- Entry/Exit Point Parameters.
- Access Codes Parameters.
- User names, passwords, access levels.
- System status.

5. Proximity Card Reading Sensor

The proximity card reading sensors should connect to the control units via data lines. It shall detect command key codes when the key is within specified range from it.

The sensor shall read data encoded on proximity cards containing tuned circuits placed within the read range of the sensor and should not require any contact of the cards with the sensor.

It shall be totally sealed, weather proof, water resistant and tamper proof. The Card reader shall be mounted in a rugged weatherised polycarbonate housing to withstand harsh environments & provide a high degree vandal of resistance.

It shall be suitable to operate within relative humidity of 0% to 100% and temperature range of -30° C to + 65° C.

The Sensor shall be capable of being mounted on wall to ensure read from a minimum specified range. The sensor should have the capacity of being mounted behind any nonmetallic, non-conductive surface including glass.

When the proximity card is presented to the reader, the red LED shall flash green and beeper shall sound.

6. Proximity Cards

The Card shall have numeric encoded data in the form of passive tuned circuits within the card. Each card shall be encoded so that it is totally unique and exists in no other system. It shall have the capability to be programmed to operate at different locations.

The Card should be capable of generating an access number consisting of eight digits. It shall be made of heavy duty fibre glass epoxy with vinyl covering. It should be credit size and highly resistant to abrasion or bending.

The key should operate in temperatures ranging from - 30 degrees C - + 65 degrees C and from 0% - 100% relative humidity. The power for the card should be generated from the sensor.

7. System Software

The System software for the Access Control System shall be powerful and multifunctional. It shall be window based and shall be flexible to allow upgradation as and when new version of software is released.

It shall operate on a high quality computer based on the 486 processor or higher.

The Access control System Software shall be designed to grow as the project needs grow. Modular software shall allow for future system features to be added as management recognizes requirements.

- **Operator Interface/Operations**

  The system software shall fulfill the following requirements for operator monitoring and command functions:-

  - ❖ Menu driven screen selection shall allow even an infrequent operator to move through and manage the functions of the system easily and with a minimum of training. There shall also be no need to memorise complicated commands or procedures.

  - ❖ Function key control of actions must provide the ability to control the system with simple key strokes.

- **System Password Protection/Control**

  - ❖ Operator and password shall control access to all menus and screens and the corresponding capability of each screen.

  - ❖ The system shall be able to assign each and every operator a completely unique set of capabilities. The system shall protect the password screen by blanking out the password when the operator enters it.

- **Real Time Reporting & Display**

  The system shall process inputs in real time, using priority levels defined by the System Administrator. The System Administrator shall have the capability to assign priority levels.

  The system shall associate graphic maps with monitor points and must display maps in real time.

- **Real Time Status Reports**

  System status reports shall be available by monitoring device category and access category.

- **Override Command Capability**

  The system shall provide the operator the liability, based on pass word authorization to override pre set conditions. The override shall include:

  - ❖ Unlock/relock entry/exit points
  - ❖ Shunt/Unshunt monitor points
  - ❖ Open, limit or close the areas covered by specific controllers.

- **Graphics for Maps**

Using simple keys to facilitate selection and placement of graphic symbols. The system should defines maps representative of site. The symbols should be associated with monitor points.

- **Diagnostics**

  The software shall provide operators with the ability to examine the status of the system components and communications.

- **Audit Trail of All Operator Activity**

  The System Administrator shall be provided with the ability to the monitor and manage all actions performed by operators on the system. Audit trial records shall be saved to hard disk and not be able to be modified. The only possible actions for audit records shall be report retrieval and archiving for off line storage.

- **System Management**

  The software shall allow the system to perform the following functions:

  - ❖ The host computer shall provide control of all system administration functions via menu accessed screens. There shall be no need to memories complicated commands or to learn the syntax of the DOS operating system. System administrative functions shall include.
  - ❖ Adding and deleting system users and their passwords.
  - ❖ Performing system and database backups.
  - ❖ Displaying current system activity.
  - ❖ Performing transaction archives.
  - ❖ Initiating data transfer to remote devices.
  - ❖ Defining and maintaining user controlled fields
  - ❖ Performing alarm transaction cleanup.
  - ❖ The system shall define
  - ❖ Access control/security panic monitoring devices
  - ❖ Communication characteristics.
  - ❖ Grouping of doors and monitor points
  - ❖ Defining readers.
  - ❖ Defining reports.
  - ❖ Defining Card Numbers, Names, Cards Validity Dates & Expiration Dates.
  - ❖ Defining time periods/holidays.
  - ❖ Defining data grouping such as group time periods, doors, monitor points and key holders to ease data entry.
  - ❖ Data base Download to distributed Workstations

The host computer shall download all information pertinent to particular control unit. The System shall execute downloads automatically at predefined times or by manual activation.

- Reports

The System shall be able to execute reports without impacting the real time operation of the system. The System shall track and real time operation of the system. The System shall track and report the dates archived events available for reporting. It shall be able to generate reports for activity any time period.

The System shall separate reports by groups and shall provide reports for every data line maintained in the system.

The following predefined reports shall be available:

- Detail activity on the system within specified time intervals.
- Provide selective reporting of specific types of activity on the system within specified time intervals.
- Any time data is changed the system shall maintain an audit trail of the data changed and who made the change.

- Online Storage of Events

When the data base approaches a certain percentage of its limit, the system shall issue an alert to inform the operator of the condition and recommend that the operator perform an archive to floppy disk.

- Archiving Event

The system shall provide the ability to backup to floppy disk all events stored in the transaction file . In the events of hardware failure or need to execute a report using archived events must be able to be restored to the system.

- Backup Restoration of System Definition

The System shall provide the ability to backup to floppy disk definition, including both hardware and user information. In the data corruption, tampering or other loss of data integrity, the system definition shall be able to be restored to the Online System from the floppy disk.

- Access Control Operation

The Software shall capture all events that occur at installed access controllers and such event capture shall occur real time. The software shall provide the ability automatically to change state of certain devices or areas based on time.

If for any reason communication between the host computer and the access controllers is interrupted the controller shall continue to make its own decisions. While connected to the host computer, the system shall continuously update the controllers with necessary information to operate in fail soft mode.

The Software shall provide capability to trace activity of card holders at specific entry/exit points. The System shall provide a display that summarizes the current condition of all the monitor points.

- Security Management Operation

The Software shall capture all events that occur at installed panic buttons and such event capture shall occur real time.

The event capture shall be reported to the host computer and the event updated on the layout maps on a real time basis.

The Software shall provide capability to display status of panic buttons.

The Software shall be upgradeable to take on additional monitor points and access controllers as required from time to time. It shall also be upgradeable for real time control of CCTV system.

The Software should be capable of recording all events of the Fire Detection and Alarm system as installed by the Client.

C. IP C.C.T.V. System

1. Scope

This section covers the design, supply, installing, testing and commissioning of Closed Circuit Television system comprising Cameras, recorder, switches and monitors.

- The IP camera family shall include a choice of
  - ❖ Fixed-format Mega pixel dome models.
  - ❖ Fixed-format Mega pixel Bullet models.

- Fixed-format High resolution dome models. These IP cameras shall offer M-JPEG, H.264 and MPEG-4 video compression in order to align with or optimize network bandwidth and video storage provisioning.

- These IP cameras shall include megapixel-resolution models, and shall offer several lens options.

- The Megapixel-resolution IP cameras shall be supplied with Megapixel lenses. The housing enclosure for megapixel cameras shall be IP66 compliant. Suitable mounting accessories are supplied as per the mounting needs.

- All cameras shall support a Power over Ethernet (PoE) interface.

- The dome cameras shall offer a sensor based true wide dynamic range of 100 db.

- The bullet cameras shall offer a sensor based true wide dynamic range of 100db.

- The cameras shall be capable of generating (At Least) up to 2 simultaneous video streams, with the following attributes:

  - ❖ Individual camera feeds shall be recorded by the VMS at different compression, resolution and capture rate settings simultaneously.

  - ❖ An adaptive transmission algorithm shall throttle these video streams to a preset maximum data rate or scale that rate based on variable network bandwidth available at the time of transmission.

- All IP cameras shall provide backlight compensation.

1. IP Dome Cameras

- Camera Type IP Dome Camera
- Sensor 1/2.8", 2.0 megapixel, progressive scan, CMOS
- Lens - 2.8 ~ 12mm@ F1.6
- True WDR up to 120dB at Full Resolution
- Illumination - Colour: 0.002Lux (F1.6, AGC ON), 0 Lux with IR
- Up to 30m (98ft) IR range
- IR ON/OFF – Auto / Manual
- Shutter - Auto/Manual, 1 ~ 1/100000s
- Defog – Digital defog
- True Day/Night Functionality IR-cut filter with auto switch (ICR)
- Video Compression - 265, H.264, MJPEG
- Frame Rate - Main Stream: 2MP (1920*1080), Max 30fps; Sub Stream: 2MP (1920*1080), Max 30fps; Third Stream: D1 (720*576), Max 30fps
- H.264 code profile - Baseline profile, Main Profile, High Profile
- Video Bit rate - 128 Kbps~16 Mbps
- 9:16 Corridor Mode – Supported
- Privacy Mask, Motion Detection, Flexible Cropping, Bit Rate, Control, Multi-Streaming, Multicasting, and Forensic Zooming
- Total Power Over Ethernet (PoE) Solution
- Audio compression, 2 way audio, suppression supported, sampling rate-8khz
- Digital noise reduction - 2D/3D DNR
- Flip - Normal/Vertical/Horizontal/180°/90°Clockwise/90°Anti-clockwise
- Compression Type H.264 (MPEG-4, Part 10) / Motion JPEG
- Network Protocols RTSP, RTP/TCP, RTP/UDP, HTTP, DHCP, TFTP, QoS, IPv4, IPv6, 802.1x
- Industry Standard ONVIF (Profile S, Profile G, Profile T), API
- Certification - CE: EN 60950-1, UL: UL60950-1, FCC: FCC Part 15
- Real-time Motion Detection
- Backlight Compensation
- IP66, IK-10,12VDC/24VAC/PoE

2. IP Bullet Cameras

- Camera Type IP Indoor Bullet Camera
- Sensor 1/2.8", 2.0 megapixel, progressive scan, CMOS
- Lens - 2.8 ~ 12mm@F1.6
- True WDR up to 120dB at Full Resolution
- Illumination - Colour: 0.002Lux (F1.6, AGC ON), 0 Lux with IR
- Up to 50m (164ft) IR range
- IR ON/OFF – Auto / Manual
- Shutter - Auto/Manual, 1 ~ 1/100000s
- Defog – Digital defog
- True Day/Night Functionality IR-cut filter with auto switch (ICR)
- Video Compression - 265, H.264, MJPEG
- Frame Rate - Main Stream: 2MP (1920*1080), Max 30fps; Sub Stream: 2MP (1920*1080), Max 30fps; Third Stream: D1 (720*576), Max 30fps
- H.264 code profile - Baseline profile, Main Profile, High Profile
- Video Bit rate - 128 Kbps~16 Mbps
- 9:16 Corridor Mode – Supported

- Privacy Mask, Motion Detection, Flexible Cropping, Bit Rate, Control, Multi-Streaming, Multicasting, and Forensic Zooming
- Total Power Over Ethernet (PoE) Solution
- Audio compression, 2 way audio, suppression supported, sampling rate-8khz
- Digital noise reduction - 2D/3D DNR
- Flip - Normal/Vertical/Horizontal/180°/90°Clockwise/90°Anti-clockwise
- Compression Type H.264 (MPEG-4, Part 10) / Motion JPEG
- Network Protocols RTSP, RTP/TCP, RTP/UDP, HTTP, DHCP, TFTP, QoS, IPv4, IPv6, 802.1x
- Industry Standard ONVIF (Profile S, Profile G, Profile T), API
- Certification - CE: EN 60950-1, UL: UL60950-1, FCC: FCC Part 15
- Real-time Motion Detection
- Backlight Compensation
- IP66, IK-10,12VDC/24VAC/PoE.

3. Server Storage NVR

- IP Video Input - 32-ch
- Two-way Audio Input - 1-ch, RCA
- Incoming Bandwidth- - 320 Mbps
- Remote Users – 128
- Protocols - SNMP,P2P, UPnP, NTP, DHCP, PPPoE
- HDMI/VGA Output - HDMI1/VGA: 1920x1080p /60Hz, 1920x1080p /50Hz, 1600x1200 /60Hz, 1280x1024 /60Hz, 1280x720 /60Hz, 1024x768 /60Hz, HDMI2: 4K (3840x2160) /60Hz
- CVBS Output - 1-ch, BNC
- Recording Resolution - 5MP/4MP/3MP/1080p/960p/720p/D1/2CIF/CIF
- Audio Output - 1-ch, RCA
- Synchronous Playback - 16-ch
- Corridor Mode Screen - 3/4/5/7/9/10/12/16/32
- Decoding format - H.265, H.264
- Live view/ Playback 5MP/4MP/3MP/1080p/960p/720p/D1/2CIF/CIF
- Capability - 3 x 12MP@25, 4 x 4K@30, 8 x 4MP@30, 16 x 1080P@30, 32 x 960P@25, 36 x 720P@30, 64 x D1
- Hard disk SATA - 8 SATA interfaces
- Capacity - Up to 10TB for each HDD
- eSATA – 1 eSATA interface
- VCA Detection - Face detection, Intrusion detection, Cross line detection, Audio detection, Defocus detection, Scene change detection, Auto tracking
- VCA Search - Face search, Behavior search
- Statistical Analysis **-** People counting
- Array Type - RAID 0, 1, 5, 6, 10
- Network Interface - 2 RJ45 10M/100M/1000M self-adaptive Ethernet Interfaces
- Serial Interface - 1 x RS232, 1 x RS485
- USB Interface - Rear panel: 2 x USB2.0, 1 x USB3.0
- Alarm In – 16 ch
- Alarm out – 4 ch

5. Layer-2 PoE Distribution Switch

- **General Features & Performance**

- Rack Mountable
- Minimum switching capacity: 216 Gbps or more
- Minimum forwarding rate: 130 Mpps or more
- Minimum DRAM 512 MB and 128 MB Flash
- Should support internal redundant power supply
- Should provide wire-speed and non-blocking performance on all the ports
- Minimum IPv4 & IPv6 Routes : 250
- MAC addresses support: 16,000
- VLANs support: 1000 active VLANs
- Should be IPv6 ready from day 1
- Should support IEEE 802.3az EEE (Energy Efficient Ethernet)
- Should support 9K or higher Jumbo frames
- Should support minimum 8 ports in a single Ether Channel group or equivalent protocol for Bandwidth aggregation.
- Should have Net Flow or sFlow from day one.

- **Interfaces**

  - Minimum of 24 x 10/100/1000 BaseT POE+ RJ 45 Ethernet Ports (must provide POE+ power on all 24 ports simultaneously).
  - Minimum 4x 10GBaseX SFP+ ports for uplinks
  - Should have dedicated flexstack or equivalent stacking with minimum 80 Gbpsvia 40G ports or more Stacking bandwidth to stack up to 8 switches into a single virtual switch. Necessary stacking modules / ports / cables needs to be supplied from day 1.
  - Should support sub 50ms ring protection as per IEEE 802.17/equivalent protocol.

- **Layer-II Features**

  - Should support IEEE 802.1Q VLAN encapsulation
  - Should support 802.1d, 802.1s, 802.1w & 802.3ad protocols
  - Should support Spanning-tree root guard to prevent other edge switches becoming the root bridge
  - Should support PVST / PVST+ or equivalent spanning tree protocol
  - Should support Unidirectional Link Detection Protocol (UDLD) or equivalent protocol to allow unidirectional links failure detection
  - Should support Link Layer Discovery Protocol (LLDP) / CDP or equivalent protocol
  - Should have Layer 2 IEEE 802.1p (class of service [CoS]), 8 hardware queues per port, Per-port QoS configuration, Differentiated services code point (DSCP) marking, CoS-based egress queuing, Egress strict-priority queuing and ACL-based QoS classification (Layers 2, 3, and 4)
  - Should support IGMP snooping v1, v2 & v3

- **Security**

  - RADIUS / TACACS, which allows centralized control of the switch and restrict unauthorized users from altering the configuration
  - Should support IEEE 802.1x to provide port-based user authentication
  - Should support port security and Secure Shell (SSH)

- **Management**

  - Should have a Manageability through a common network-management software on a per-port and per-switch basis
  - Should support SNMP versions 1, 2, and 3 and RMON
  - Should support Network Time Protocol (NTP)
  - Configuration through the CLI, console, Telnet, SSH and Web Management
  - Should support Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location
  - Should have dedicated out of band 10/100/1000 base Ethernet port and dedicated serial console port.

III. PREFACE

C. Tropical Conditions

All equipment/material supplied against respective Specification shall be suitable for satisfactory continuous operation, storage & maintenance under tropical conditions as specified below:

- Ambient temperature : 45 degree Celsius
- Annual Average Relative humidity : 50%
- Isokeraunic level (days per year) : 50
- Seismic Zone : Zone-4
- Climate type : Moderately hot and humid tropical, climate, conducive to rust and fungus growth

D. Tolerance and Creepage Distances

Tolerances (on all the dimensions) and creepage distances shall be in accordance with provisions made in the relevant Indian/IEC/BIS standards and in these specifications. Otherwise the same will be governed by good engineering practice in conformity with required quality of the product.

IV. Special Points for Passive Components:

- All copper & Fiber component should be from single OEM as per the makes given in the tender documents.
- All passive components should be RoHS (Restriction of Certain Hazardous Substances) complied. Declaration-RoHS Should be clearly mentioned on datasheet of each Passive Component.
- The manufacturer of Passive component should be a technology development partner with any of the leading Manufacturer of Active Component.
- Bidder has to submit an authorization letter from the OEM only specific to this work. All bids without the authorization letter will be liable to be rejected.
- All work related to fiber including digging, laying of HDPE Pipe/Hume Pipe/Conducting will be in the bidders

scope. The Bidder Should take in consideration all the cost involved for the same, nothing shall be paid extra on account for this.

- Bidder has to support the complete system for one year after the completing the installation and assign one dedicated resource for the same for one year on their own cost only.
- Bidder should have adequate facilities, manpower and staff for installation testing and commissioning and can provide after sales services. OEM has to authorize their System Integrator in this regards stating that they will Support the solution through their SI.

13. OEM Eligibility Criteria for Passive Products

Sr. No.	Eligibility Criteria	Compliance with Document
1	OEM of Passive Networking Products must be registered in India for more than 15 years.	
2	OEM of Passive Networking Products shall have their own ISO 9001:2008 and 14001 certified copper and fiber components manufacturing facility in India.	
3	OEM of Passive Products should have atleast 1 RCDD Residing in India is preferred.	
4	OEM must not propose any mix of Co-branded equipment. All Products (Cat6 and Fiber) shall be of same brand name written on each quoted product.	
5	All the Passive Products (Cat6 and Fiber) Shall be from Single OEM & offered products should have Min. 25 years of performance warranty.	
6	OEM shall be TIA Full Committee Member and its name shall be available on TIA Website.	

14. CAT6 U/UTP 4 Pair LSZH CABLE

Details	Specification	Compliance
Type	23 AWG Solid Bare Copper, Unshielded Twisted 4 Pair, Category 6, TIA / EIA 568-2.D, ISO/IEC 11801 & NEC Articles UL 444.	
Application	Premise Horizontal Cable, Gigabit Ethernet, 100BaseTX, 100BaseVG ANYLAN, 155ATM, 622ATM, NTSC/PAL Component or Composite Video, AES/EBU, Digital Video, RS-422, 250MHz Category 6, IEEE 802.3bt Type 1, Type 2, Type 3, Type 4	

Details	Specification	Compliance
Conductors	Solid Bare Copper	
Insulation	Polyethylene / Polyolefin	
Jacket	LSZH jacket complying to: Fire rating IEC 60332-1 Toxicity IEC 60754-1 Smoke density IEC 61034-1	
Pair Separator	Cross-member **(+)** fluted Spline.	
ETL Test Report	ETL Transmission Test Report as per ANSI/TIA-568.2-D Min. 250 MHz to be provided with Minimum 4 Connector Channel NEXT Headroom of 3dB.	
Packing	Box of 305 meters	
Cable Outer Diameter	5.8 mm	
Propagation Delay Skew	≤ 45ns/100m or Better (ETL/UL Tested)	
Bend Radius	4 * Cable Diameter	
Impedance	100 Ohms + / - 15 ohms,	
Maximum Capacitance	ETL Report to be submitted for below parameters:- Max. Capacitance Unbalance: ≤ 20 pF/100 Mtr Max. Mutual Capacitance :- ≤ 5.0 nF/100m	
Max. DCR	<= 7.3 Ohms Max /100 mtr (ETL/UL Tested)	
PoE Capability	IEEE 802.3bt Type 1, Type 2, Type 3, Type 4	

Details	Specification	Compliance
Performance characteristics as per ANSI/TIA-568.2-D	Max. Attenuation: 32.8dB/100m Min. NEXT : 38.3 dB Min. PS NEXT : 36.3 dB Min. ELFEXT : 19.8 dB Min. PSELFEXT : 16.8 dB Min. Return Loss: 17.3 dB Min. ACR : 5.5 dB Min. PSACR :3.5 dB	
ROHS Compliant	ROHS/ELV Compliant	
Operating Temperature Range	-20 to +75 Deg C	
Test Reports	Test Reports from any NABL Accredited Lab needs to be submitted for below test at time of bidding.. 1. Oxygen Index Test 2. Smoke Density Test 3. Halogen Acid Test with Acidity & Conductivity Test 4. Vertical Flame Test IEC 60332-1 5. Temperature Index Test	

15. Cat 6 Unshielded Modular Jack (without PCB)

Parameters	Specifications	Compliance
Type	Cat6 Modular Jacks shall meet and exceed channel specification of Category 6 transmission requirements for connecting hardware, as specified in Commercial building telecommunications Cabling standard and ISO/IEC 11801:2002 second edition. when used as a component in a properly installed UTP channel.	
Front Connection	Lead Frame : Copper Allow with 50u inch Gold over Nickel	
Rear Connection	IDC: Copper Alloy with Nickel Plating	

Parameters	Specifications	Compliance
Connector Body	Plastic: UL940V-0	
Housing	Encapsulated Lead Frame technology (Without PCB)	
Accessories	-Jack should support uniform hassle free termination technology and be able to ensure performance in each termination without dependency on expertise of technician. - Integrated bend-limiting strain-relief unit for cable entry with locking facility at IDC contact point	
Termination Interface	Front Mated Connection: 750 Cycles or Better	
	Rear Mated Connection: 20 Cycles (Gas Tight IDC Connection) or Better	
Jack Details	Connector/hardware retention of at least 88.5 N Plug /connector retention of at least 50N Storage temperature range of -40 Deg C to +70 Deg C.	
IEEE Specification (PoE)	IEEE 802.3at type 1 and 2 (up to 30W). CoC to be provided.	
Termination Pattern	TIA / EIA 568 A and B	
Performance	1 Gbps support for 100 MT Channel Link	
Guaranteed Bandwidth	250 Mhz Guaranteed Bandwidth for 100 MT Channel Link	
Approvals (Proof to be provided along with Bid)	UL Listed	
	ETL verified to TIA / EIA Cat 6. Should be part of the registered 4 connector channel as per Intertek / ETL report	
UL Rating	UL 94V-0	
Other Specifications	UL 1863, IEC 60603-7, FCC part 68-F	
RoHS	Compliant	
Feature	The jacks shall not have an integrated spring shutter as the shutter malfunctions and causes operational issues in Panel.	
Safety listing	ACA and Bi-national standard listed.	
Operating Temperature	-10° to 60°C	
Dielectric Strength	1,000 V RMS @ 60 Hz for 1 minute (Signals to Ground)	
Termination Process	Termination of cable on IO through Termination Tool to minimize any manual termination like punch down. All the four pairs should get crimped and cut together with	

Parameters	Specifications	Compliance
	the help of the tool. Pairs should be separated via mechanism in the termination process to avoid any cross talk issue at Jack. Tool-less jack is not required because the tool-less jack is installer dependent, whereas the termination using a tool has consistent terminations ir-respective of the installer.	
Cat6 Jack	Should be covered under 25 year warranted solution from OEM. All the four pairs should get crimped and cut together with the help of the tool.	

16. Cat 6 Unshielded Patch Cords, LSZH, ETL Tested

Details	Specification	Compliance
Type	Unshielded Twisted Pair, Category 6, TIA / EIA 568-C.2 & ISO/IEC 11801, IEC 60603-7, FCC Part 68 Subpart F Specifications.	
Conductor	Cat6 Patch Cord should be 4 Twisted Pair, 24 AWG Stranded Bare Copper Conductors. Contact Blade should be Phosphor bronze plated with 50u'' gold over 100u'' nickel undercoat.	
Length	1 MT , 3 MT	
Plug Protection	Factory fitted Strain relief boots on either side	
Performance Characteristics	Max. Current Rating should be 1.5 Amp Min. Insulation Resistance should be 500MOhm Max. Contact Resistance should be 20mOhm Dielectric Strength should be 1000 VAC (RMS)	
Jacket	LSZH	
Outer Diameter	≤ 6.0 mm	
Operating Environment Range	The patch cord should have Insertion Life of 750 mating cycles	

Details	Specification	Compliance
	Pull force of min. 89 Newton, Operating Temperature range of -20 Deg C to +60 Deg C	
Boot	Clear / Transparent with Snagless feature	
Third Party Verification	4 Connector ETL/UL Test Report 600 Mhz for ANSI/TIA-568-2.D needs to be submitted along with bid. This Patch Cord shall be part of ETL/UL test report of 4 connector channel submitted for quoted Cat6 cable.	

17. CAT6A U/UTP LSZH CABLE

Details	Specification	Compliance
Type	23 AWG Solid Bare Copper, Unshielded Twisted 4 Pair, Category 6A, confirming to TIA 568.2.D, Class EA - ISO/IEC 11801:2002	
Conductors	Solid Bare Copper 23 AWG	
Insulation	Polyolefin/Poylethylene	
Jacket	LSZH jacket complying to: Acid Gas Emission pH per IEC 60754-1 : ≥ 4.3 Acid Gas Conductivity per IEC 60754-2 : ≤ 10µs/mm Smoke density IEC 61034-2 : ≥ 60% Light Transmittance Flame Test: IEC 60332-1 Third Party Test Report of above parameters needs to be enclosed with bid.	
Pair Separator	+ Shape Spline	
Suitable Applications:	Premise Horizontal Cable, 10 Gigabit Ethernet, 100BaseTX, 100BaseVG ANYLAN, 155ATM, 622ATM, NTSC/PAL Component or Composite Video, AES/EBU Digital Audio, AES51, RS-422, Noisy Environments, PoE	
Guaranteed Bandwidth	500 Mhz for 100 MT Channel	
Packing	Box of 305 meters	
Cable Nominal Outer Diameter	7.2 mm	
Max. Delay Skew	45 ns @ 100M	

Details	Specification	Compliance
Bend Radius (Installation)	50 mm	
Maximum Conductor DC Resistance:	DCR @ 20°C (Ohm/100 m) < 8.0	
Third Party Verification for Cable	Cable ETL Test Report for compliance to 61156-5 as referenced in ISO/IEC 11801-1 for Min. 500Mhz or Higher Cable ETL Test Report for Alien crosstalk for ANEXT, AFEXT, PS ANEXT. All above test reports to be submitted along with bid	
Nom. Mutual Capacitance	Capacitance (nF/km) < 56	
Nom. Velocity of Propagation	67 % or Better	
Temperature Range Operation	-20 Deg C to +60 Deg C	
IEEE Requirement	IEEE 802.3bt Type 1, Type 2, Type 3, Type 4	
RoHS	Yes	
Test Report	Enclose ETL 4 Connector Channel Test Report as per ANSI/TIA-568.2-D Category 6A Standard.	

18. Cat 6A Unshielded Modular Jack

Parameters	Specifications	Compliance
Type	Modular Jacks shall meet and exceed channel specification of ANSI/TIA/EIA-568-C.2 Category 6a and ISO/IEC 11801:2002/Amd 1:2002 Ed2 when used as a component in a properly installed UTP channel.	
Front Connection	RJ 45 : 50uin Gold plated contacts over Nickel	
Rear Connection	Copper alloy, Gold plated contacts over Nickel or IDC	
Connector Body	PBT glass reinforced UL94V-0 or Plastic	

Parameters	Specifications	Compliance
Accessories	Jack should support uniform hassle free termination technology and be able to ensure performance in each termination without dependency on expertise of technician.	
Termination Interface	Front Mated Connection: 750 Cycles Min.	
	Rear Mated Connection: 20 Cycles Min.	
IEEE Specification (PoE)	IEEE 802.3bt type 3 and 4 (up to 100W)	
	Cisco UPOE (up to 60W) and Power over HDBase-T (up to 100W)	
Performance tests	Modular Jacks shall be tested for performance to ANSI/TIA/EIA-568-C.2	
Guaranteed Bandwidth	Min. 500 Mhz or higher Guaranteed Bandwidth for 100 MT Channel Link	
Approvals	UL Listed, UL2043 Air Handling Spaces	
UL Rating	UL 94V-0	
Other Specifications	UL 1863, IEC 60603-7, FCC part 68-F	
RoHS	EU Directive 2002/95/EC Compliant	
Feature	The jacks shall not have an integrated spring shutter as the shutter malfunctions and causes operational issues in Panel.	
Operating Temperature	-10° to 60°C	
Dielectric Strength	1,000 V RMS @ 60 Hz for 1 minute (Signals to Ground)	
Termination Process	Termination of cable on IO through Universal Termination Tool to minimize any manual termination like punch down. All the four pairs should get crimped and cut together with the help of the tool. Pairs should not be separated in termination process to avoid any cross talk issue at Jack. Tool-less jack is not required because the tool-less jack is installer dependent, whereas the termination using a tool has consistent terminations ir-respective of the installer.	
Cat6A Jack	It should be covered under 25 year warranted solution from OEM.	
Third Party Test Report	Enclose 4 Connector ETL/UL/3P Test Report ANSI/TIA – 568 Cat6 6A, ISO/IEC 11801 (Class Ea), EN 50173 (Class Ea) and IEEE 802.3-2012.	

19. Cat 6A Unshielded Patch Cords, LSZH

Parameters	Specifications	Compliance
Type	Modular Cord shall meet and exceed channel specification of ANSI/TIA/EIA-568-B.2 Category 6a and ISO/IEC 11801 2nd edition (2002) & Amendment 2 (2010) up to 500 MHz when used as a component in a properly installed UTP channel. It should also comply to EN 50173-1 (2002) & EN 50173-1 Amendment 1 (2009).	
Conductor	Stranded copper, 7/26AWG	
Insulation	Foam Polyethylene/PE	
Plug Boot	Clear boot with PVC material, Snagless	
Plug Housing	Polycarbonate (PC)	
Plug contact blade	Phosphor bronze plated with 1.27um gold over 2.54um nickel undercoat	
Insertion Life	750 Cycles or Better	
Operating/Storage Temperature Range	-20 to +60 Deg C	
Channel compliance certificate	Certificate by Intertek (ETL)/UL/3P for the 4-Connectors and 3 Connectors channel testing to the Cat 6A Cabling system as per the ANSI/TIA 568 C.2 standards, ISO/IEC 11801 and EN 50173-1. Document to be submitted.	
Guaranteed Bandwidth	500 Mhz or Better Guaranteed Bandwidth	
Sheath Material	LSZH	
Flame Rating	IEC 60332-3 or higher	
Outer Diameter (Nominal)	6.1 ± 0.3 mm	

20. 24 Port, 1U Jack Panel, Unloaded (For Cat6 and Cat6A)

Parameters	Specifications	Compliance
Type	- 24 Port 1RU Unloaded Straight Patch Panel - 19" rack mountable. - Patch panels Ports should be individually replaceable & Consistent port-to-port performance.	

Ports	24 Ports in 1RU and 48 Ports in 2RU	
Cable management	Panel shall have in-built cable manager at the rear end	
Height	1U (1.75")	
Feature	The jacks shall not have an integrated spring shutter as the shutter malfunctions and causes operational issues in panels.	
Storage Temperature Range	-40Deg C to +70 Deg C	
Operating Temperature range	-10Deg C to +60 Deg C	
Color and Material	Black Color SPCC Steel Frame Material with ABS Front Plastic Panel	
RoHS	EU Directive 2011/65/EU (ROHS II)	

21. Face Plate, UK Style, 6C Type, White Color, Square with Shutters

Details	Specification	Compliance
Type	**Simplex/Duplex/Quad**	
Material	Fire -retardant Plastic UL-94 V0, ABS, UK Style.	
Acceptability	Should be able to accept Cat6A, Cat6 and Cat5e information outlets	
Mounting screws	2 pcs, M3.5 x 25mm	
Compliant	RoHS	
Dimensions	(H x W x D) 86 x 86 x 10 mm	

22. 6/12 Core Single mode Outdoor Armored Fiber Cable

Details	Specification	Compliance
Cable	12 Core Singlemode 9/125, Central Loose Tube Cables, High mechanical and rodent protection provided for Outdoor – Corrugated Steel Tape Armor (CST), complying to 9/125 ITU G.652D	

Details	Specification	Compliance
Application	Cable should be suitable for Structured (premises) wiring systems: For outdoor use in structured (data) wiring systems such as industrial backbone, campus backbone, building backbone (riser). Suitable for direct burial. Easy to install in ducts, tunnels and trenches.	
Jacket	Black UV resistant HDPE outer jacket. Glass yarns and two steel wires embedded in jacket as strength members.	
Loose Tube Construction	Central tube, jelly filled (non-dripping and silicon-free) with up to 12 fibers. Individually colour coded optical fibres.	
Optical Properties	Core: 9.2 +/- 0.4 um Cladding: 125 +/- 0.7 um Loose Tube fibres: Ø 250 ± 15 µm 1310 Wavelength (nm) : 0.36 Attenuation max. (dB/km) 1550 Wavelength (nm) : 0.22 Attenuation max. (dB/km) Zero Dispersion Wavelength : 1302 – 1322 nm Core-Clad Concentricity Error : ≤ 0.5 µm Clad Non-Circularity : ≤ 0.7 % Cutoff Wavelength : ≤ 1260 nm PMD (ps/km) : ≤ 0.1 Point Loss @ 1310nm & 1550nm : 0.05 dB Refractive Index @1310nm : 1.467 Refractive Index @1550nm : 1.468	
Warranty & Putup	Std. delivery length: 2000 ± 105m Minimum Warranty: 25 years.	
Temperature Range	-40 to +70 °C	
Physical Properties	Bending radii tube (Installation & Operation) : 20 x OD mm Cable Max. Tensile Strength Installation (Short Term): 2000 N Cable Max. Crush Resistance Installation (Short Term): 3000 N/100mm Nominal Cable OD : 9.2 mm Max.	

Details	Specification	Compliance
	RoHS for Outer Jacket Buffer Tube Material : PBT – Polybutylene Terephthalate	

23. 12/24 Fiber Port 1U Rack Mount Fiber Enclosure (LIU) including Splice Trays, Pigtails and Couplers

Details	Specification	Compliance
Fiber Interface Unit	Fiber Patch Panel Typically used in Server rooms, Network rooms, Data Centres and Small offices Can be mounted directly on any 19" rack or cabinet. It should be able to accommodate a variety of Fiber connectors and terminated to fiber cables using Splicing or other methods.	
Type	Fiber LIU should be 1U (1.75”), 19 Inch Rack Mount.	
	12/24/48Fiber Port should be available in 1U Rack Mount LIU.	
	LC Type Connectors will be required.	
Features & Compatibility	Each 1U LIU should be able to accommodate atleast 48 fibers in LC type connectors.	
	12/24/48 Fiber Splice trays should loaded in LIU with Pigtails, Splice Tubes, Min. 2 x PG13.5 Gland, Cable Ties and Velcro Straps	
	Panel Material – Powdered Coated Steel	
	Couplers in adapter strip should be colored to specify OM4 and shall meet Pigtail and Patch Cord Color	
	Operating Temp Range: -10^{o}C to +60^{o}C	
	Storage Temp Range: -40^{o}C to +70^{o}C	
	EU Directive 2011/65/EU (ROHS II)	
Pigtails Parameters factory loaded in Panel	LC - Simplex, Singlemode OS2, Min. 2 Mtr, 0.9mm Tight Buffer	
Standard	Optical Fiber Pigtail should comply with TIA 568.3-D	
Optical Performance	Insertion Loss of <=0.30dB	
Optical Performance	Return Loss of ≥ 55dB	
Connector Standard	IEC 61754, TIA 604	
RoHS	EU Directive 2011/65/EU (ROHS II)	

24. Fiber Patch Cords, LC-LC Duplex, Singlemode OS2, 3MT

Details	Specification	Compliance
Type	2mm Duplex Zipcord or Better Singlemode OS2	
Outside Diameter	(Duplex): 2.0mm or Better	
Jacket Material	LSZH	
Length	3 MT	
Cable Crush Resistance	500 N/100mm	
Insertion Loss	≤ 0.30 dB	
Return Loss	≥ 55dB	
RoHS Certified	Yes	
Cable/Connector Standard	IEC 61754, TIA 604, TIA 568.3 D, IEC 60793-2-10, IEC 60793-2-50	
Flame Standard for LSZH	IEC 60332, IEC 60794-2-50, IEC 60754, IEC 61034	
ANSI/TIA	ANSI/TIA-568.3-D (shall be mentioned in data sheet)	

DATA IT (ACTIVE NETWORK COMPONENTS)

Special Condition for System Integrator:

The Contractor will supply and install the equipment necessary to meet the requirements and provide all labour and materials, whether or not described in full, necessary to produce complete and fully operational systems in accordance with the intent of this document.

The Contractor/ Agency must familiarize himself with the site drawings and the scope of the facilities that is required in the various areas. Should ensure that agency is aware of the operational requirements under which the systems and associated facilities are to be installed and used.

All employees used by the contractor/agency to install this system must be competent technicians who are experienced in the installation and interconnection of systems.

Bidder shall be authorized by the manufacturer of the major components of the system to sell their products and initiate warranty service on the same items for this project. Manufacturing authorization letter must be submitted for this Work addressing to Client stating that bidder is authorized to provide sales and services on behalf of OEM.

In view of the above, commissioning and programming will have to be carried out to integrate all the system architecture hardware and software

Submittals:

Compliance Statement- (Mandatory)

Datasheet- (Mandatory- Relevant Pages only)

Bill of Quantity- (Mandatory)

Drawings as required

Manufacture Authorization Letter (Mandatory)

OEM Partner Certification

No Deviation Certificate (for Technical Compliance) on OEM latter head (Mandatory).

Makes and Models: - It is mandatory to provide make and model of the items and their subcomponents as has been sought in the technical bid. Please note that substituting required information by just brand name is not enough. Bidder should not quote hardware or software items which are impending End of Life or End of Support during the contractual period.

Software, Drivers and Manuals: - The bidder shall supply along with each item, all the related documents, Software Licenses and necessary media of the software loaded in the equipment without any additional cost. The media and documents shall be in English. These will include, but not restricted to, User Manual, Operation Manual, Other Software and Drivers etc.

Warranty: The Contractor/ Agency shall Warranty that all provided material and equipment will be free from defects, workmanship and will remain so, for a period of 12 months from after equipment/materials have put into the service or from date of final acceptance of system by Engineer In charge / Consultant whichever is earlier.

The Contractor/ Agency shall provide summary of all equipment's serviced quarterly during this Warranty period to facility in charge. The report shall clearly mention services rendered, parts replaced and repairs performed.

Software & Programming:

Any software, license or programming, whether or not specifically mentioned, but if required for successful installation, testing, commissioning and functioning of the all equipment and systems installed by the contractor, the same shall be in the scope of the contractor. All such software required shall be fully-loaded, genuine, latest versions, shall be as per OEM's specifications/ recommendations, shall not be trial versions or limited- feature or limited-period versions (unless the specified Model no. / Code no. means so) and shall not involve any extra or recurring cost.

The rate quoted by the contractor shall be inclusive of all such required software and programming and the contractor shall be responsible for making the entire system operational as per tender specification and no extra shall be paid to the contractor on this account.

Compatibility of System

It shall be contractor's obligation to ensure that all the software, hardware, equipment, and IT systems, including input-output connectors/ port/ terminals, are seamlessly compatible with one another. Any specific provisions, if required to be made on this account this, shall be done by the contract without compromising the performance of the IT system and without any extra cost. The rate quoted by the contractor shall be inclusive of all such required software and programming and no extra shall be paid to the contractor on this account.

The contractor shall ensure that the equipment being proposed are the prevalent models/ series of the OEM.

Technical Specification of LAN System

Core Switch

Core Switch		
S. No	Specifications	Compliance (Yes/No)
1	General Features	
2	Switch should be 1U and rack mountable in standard 19" rack.	
3	Switch / Switch's Operating System should be tested for EAL 2/NDPP or above under Common Criteria Certification .	
4	Switch should be MTCTE (Mandatory Testing & Certification Of Telecommunication Equipment) Certified and Certificate issued by TEC (Telecommunication Engineering Center), Department of Telecommunications must be submitted.	
5	Switch should be quoted with 05 years of TAC Support & 5 years Hardware Warranty with advance hardware replacement.	
6	Switch should have minimum 4 GB RAM, 4 GB Flash and 6MB packet buffer or more.	
7	Switch should support operating temperature from 00 to 450 degree celsius.	
8	Hardware Architecture	
9	Switch should have 24 Ports of 1/10G SFP+, 4 Ports of 1/10G SFP+ or 4 porand 2 x 40G or 1 x 100G QSFP28 Uplink/Stacking Ports from Day 1. Switch should support total of 4 x 40G QSFP28 or 1 x 100G QSFP28 Ports in future by installing the interface module. Switch should support 1G Base T & 10G Base-T Copper RJ-45 Transceiver to connect with any legacy device with 1Gbps port. Switch must be supplied with redundant hot swapable fan trays & dual redundant power supply.	
10	I.Switch should support physcial stacking of 200Gbps and up to 8 Switches or more in a single stack. II. Switch should also support long distance stacking upto 10KMs. III. Switch should support aggregated stacking bandwitdh of 1600Gbps or more.	
11	Switch should have the following interfaces: I. USB Type-C, RJ-45 Serial Port for Serial Console Management II. USB Type-A for external file storage III. RJ-45 Ethernet Port for Out of Band Network Management	
12	Performance	

13	Switch shall have minimum 1Tbps of switching fabric and 800 Mpps of forwarding rate.	
14	Switch shall have minimum 96K MAC Addresses and 4000 VLAN.	
15	Should support minimum 90K IPv4 and 8K IPv6 routes or more	
16	Switch shall have 8K multicast groups or more.	
17	Switch should support 512 or more STP Instances.	
18	Switch should support trunking, 32 ports per trunk & min. 256 trunk groups or more	
19	Switch must support MACSEC Protocol.	
20	Switch must support High Availability (HA) functionality using M-LAG (Multi-Chassis Link Aggregation Group)/MC-LAG (Multi-Chassis Link Aggregation Group)/ VPC (Virtual Port Channel) etc. with independent management & Control Plane	
21	Layer 2, Layer 3 & Security Features	
22	Switch should support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z, UDLD and VXLAN.	
23	Switch must have IPv4 & IPv6 routing static routing, ECMP, RIP, RIPnG, OSPFv2, OSPFv3, VRRP, VRRP-E (IPv4 & IPv6), VRRP v3 -IPv6, PIM-SM, PIM-SSM, PIM-DM, PIM-Passive (IPv4 & IPv6), MSDP, BGP4, BGP4+ (IPv6), VRF, PBR and QoS features from Day 1	
24	Switch should support RSPAN, ER-SPAN, LLDP, Configuration Archive, Replace & Roll Back.	
25	Switch shall have 802.1p class of service, marking, classification, policing and shaping and eight egress queues.	
26	Switch should support management & authentication features like sFlow or equivalent, SSHv2, SNMPv2c, SNMPv3, NTP, MAC Authentication, Web Authentication, Flex Authentication, RADIUS, Encrypted Syslog (RFC 5425), RADSEC (RFC 6614) and TACACS+ Authentication.	
27	Switch should support IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard.	
28	Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment	
29	Switch must support protection Dynamic ARP Inspection, DHCP Snooping, Protection against Denial of Service (DOS) attacks	
30	During system boots, the system's software signatures should be checked for integrity. System should capable to understand that system OS are authentic and unmodified, it should have cryptographically signed images to provide assurance that the firmware & BIOS are authentic.	
31	Switch must support Open Flow 1.3 or latest for SDN (Software Defined Networking), REST API,	

	Ansible for automation	
32	Manageability	
33	Should support manageability using on prem Centralized Management platform using Web based Graphical User Interface (GUI) and also should be remotely manageable from the Cloud.	
34	It shall support Integrated Standard based Command Line Interface (CLI), Telnet, TFTP, HTTP access to switch for management/monitoring	
35	All Switches Core, Distribution and Access Switches shall have the similar commnad line for ease of operation & maintenance	
36	Mandatory Certification & Compliance	
37	Switch shall conform to IS 13252-1 or IEC 60950-1 or IEC: 61368-1 Annex-A for Safety requirements of Information Technology Equipment as per TEC Standard. TEC certificate to be furnished along with the bid.	
38	Switch shall conform to TEC EMI EMC Standard EN 55032 Class A/B or CISPR32 Class A/B or CE Class A/B or FCC Class A/B	
39	Switch shall conform to TEC EMI EMC Standard EN/IEC 61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN 61000-4-6, EN 61000-4-11, EN 61000-4-29 Annex B and ROHS 6.	
40	OEM should not share land border with India. Declaration on the OEM letter head to be submitted for the same.	
41	OEM should have ISO 9001:2015 certification	
42	All switches, WiFi, WLC, Transceivers, AAA should be from the same OEM for better interoperatability, management and support	
43	OEM should have 7-8 RMA depots in India for faster replacements . Details to be shared on the OEM letter head.	

48 Port Non PoE Access Switch

48Port Non PoE Access Switch		
S No.	Specifications	Compliance (Yes/No)
1	Product details - Please specify	
1.1	Please mention Make, Model No. and Part Code.	

2	Architecture & Port Density	
2.1	Access Switch should provide 48 x 10/100/1G RJ45 Ports and 4x 1G/10G/25G SFP+ Slots, for Stacking/Uplinks, from Day 1.	
	Hardware, including modules, or Software, including licenses, to support all the speeds listed above, should be available from Day 1	
2.2	Should support Virtual Switching System (VSS) or Virtual Chassis (VC) or Virtual Switching Extension (VSX) or equivalent Switch Clustering/Stacking feature, where the Switch Clustering feature should combine multiple switches into a single network element. Switch should support aggregated stacking bandwidth of 800Gbps or more and 8 switches per stack or more.	
3	Performance	
3.1	Should provide Switch Fabric Bandwidth Capacity of 296 Gbps, or more.	
3.2	Should provide Packet Forwarding Capacity of 220 Mpps, or more.	
4	MAC Address and Route Table	
4.1	Should support up to 32K MAC addresses, or more.	
4.2	Should support 16K IPv4 routes and 4K IPv6 routes, or more.	
5	Physical Attributes	
5.1	Should support 4GB RAM, 8GB Flash and 4MB Packet buffer or better	
6	Layer 2 features	
6.1	Should support Jumbo Frames (up to 9K bytes).	
6.2	Should support 4K Active VLANs, with the following features;	
	Port based VLANs	
	Dual-Mode VLANs	
	MAC-based VLANs	
	Dynamic VLAN Assignment	
	Dynamic MAC-based VLAN Activation	
	Dynamic Voice VLAN Assignment	
	VLAN mapping or VLAN Translation	
6.3	Should support Spanning Tree Protocols, with the following features;	

	802.1D Spanning Tree	
	802.1W Rapid Spanning Tree Protocol (RSTP)	
	802.1s Multiple Spanning Tree	
	802.1s Multiple Spanning Tree enhancement (MSTP+)	
	Fast Port Span, Fast Uplink Span or Equivalent	
	Compatibility with PVST/PVST+, PVRST+ and PVST+ or Equivalent	
	BPDU Guard	
	Root Guard for STP & MSTP	
	Port Loop Detection	
	Spanning Tree path cost method changes	
	MSTP path-cost configuration	
6.4	Should support Link Aggregation Groups (LAG), with the following features;	
	Static LAG	
	802.3ad Link Aggregation Control Protocol (Dynamic LAG)	
	Dynamic insertion and removal of ports	
	Support for LAG between different default port speeds	
6.5	Should support 802.1q Tunneling, with the following features;	
	802.1ad (Q-in-Q) tagging	
	Q-in-Q BPDU tunneling	
	Selective Q-in-Q	
6.6	Should support Private VLANs, with the following features.	
	PVLANs with dual mode support	
	PVLAN with LAG	
6.7	Should support VLAN Registration Protocol, with the following features;	
	Multiple VLAN Registration Protocol (MVRP)	
	MVRP with Per-VLAN STP and Per-VLAN RSTP	
6.8	Should support the following features;	

	Unicast Reverse Path Forwarding (uRPF)	
	Remote Fault Notification (RFN)	
	Link Fault Signaling (LFS)	
	Uni-Directional Link Detection (UDLD) on Tagged and Untagged Ports	
	To limit Unknown Unicast Packet Flooding (UUFB)	
	Virtual Extensible LAN (VXLAN)	
7	Layer 3 features	
7.1	Should support the following IPv4 and IPv6 Layer 3 Routing features;	
	Routing Between Directly Connected Subnets	
	Host routes & Virtual Interfaces	
	IPv4 & IPv6 Static Routes	
	RIP v1/v2 & RIPng	
	ECMP	
	OSPF v2, OSPF v3	
	PIM-SM, PIM-SSM, PIM-DM, PIM passive	
	Policy Based Routing (PBR)	
	VRRP v2 & VRRP v3	
	Non-Stop Routing (NSR)	
	GRE IP Tunnels	
	IPv6 over IPv4 tunnels and VRF	
	DHCP Server	
	MSDP	
8	Quality of Service (QoS) & Traffic Management	
8.1	Should support the following Quality of Service (QoS) features;	
	ACL Mapping and Marking of ToS/DSCP (CoS)	
	ACL Mapping and Marking of 802.1p	
	ACL Mapping to Priority Queue	

	Classifying and Limiting Flows Based on TCP Flags	
	DiffServ Support	
	Honoring DSCP and 802.1p (CoS)	
	Dynamic Buffer Allocation for QoS Priorities	
	Separate QoS Queuing for Unicast and Multicast	
	Priority Queue Management using Weighted Round Robin (WRR), Strict Priority (SP), and a combination of WRR and SP	
	Priority for PFC	
8.2	Should support the following Traffic Management features;	
	ACL-based Rate Limiting	
	Traffic Policies	
	Broadcast, Multicast, and Unknown Unicast Rate Limiting	
	Inbound Rate & Outbound Rate Limiting	
	CPU Rate Limiting	
9	Software Defined Networking (SDN)	
9.1	Should support the following SDN features and functionality;	
	OpenFlow v1.0 & v1.3	
	Hybrid Switch Mode	
	Hybrid Port Mode	
	Support for Multiple Controllers	
10	Security	
10.1	Should support the following Security features;	
	Layer 3 & Layer 4 ACLs	
	Layer 2 ACLs (MAC)	
	DHCP Snooping	
	DHCP Client & Server	
	Dynamic ARP Inspection	

	Neighbor Discovery (ND) Inspection	
	Protection against Denial of Service (DoS) Attacks	
	MAC Port Security	
	RADIUS/TACACS/TACACS+	
	Secure Copy (SCP)	
	Secure Shell (SSHv2)	
	Trusted Platform Module	
	Protected Ports	
	IP Source Guard (v4 & v6)	
	IPv6 RA Guard	
	RADSEC	
10.2	The Switch should support the following Authentication features;	
	Authentication, Authorization, and Accounting (AAA)	
	802.1X Authentication and Accounting	
	MAC Authentication and Accounting	
	Web Authentication	
	802.1x with Dynamic ACL Assignment	
	802.1x with Dynamic VLAN Assignment	
	802.1x and MAC Authentication on the same port	
	802.1x Authentication with IP Source Guard Protection	
	MAC Authentication with IP Source Guard Protection	
	MAC Authentication with Dynamic VLAN Assignment	
	MAC Authentication with Dynamic ACLs	
	MAC Authentication with 802.1x	
	802.1x together with Denial of Service (DoS) Attack Protection	
	Periodic Re-authentication for MAC Authentication	
	Periodic Re-authentication for 802.1x	

11	Monitoring & Manageability	
11.1	The Switch should support the following Monitoring & Management features;	
	RSPAN	
	NTP	
	LLDP & LLDP-MED	
	Cisco Discovery Protocol (CDP) for IPv4 and IPv6 Traffic or equivalent	
	Automation with Ansible & RESTCONF	
	DHCP Auto Configuration	
	SNMP v1, v2, and v3	
	Mirroring based on Port, IP ACL, MAC ACL and VLAN	
	Configuration Archive, Replace & Roll back	
	IP DHCP binding scalability of minimum 2K Devices	
11.2	Should support Integrated Standard based Command Line Interface (CLI), Telnet, TFTP, HTTP access to switch management/monitoring.	
11.3	Should support manageability using Network Management Software with Web based Graphical User Interface (GUI) and Cloud based Management Solutions.	
11.4	Should support NetFlow or sFlow or equivalent.	
12	Mandatory Compliance & Warranty and support:	
12.1	All switches, WiFi, WLC, Transceivers, AAA should be from the same OEM for better interoperatability, management and support	
12.2	The Switch OS should be EAL/NDPP and ROHS6 Certified. Certificate needs to be enclosed along with the bid	
12.3	The Switch must be MTCTE Certified and TEC certificate shall be submitted	
12.4	The Switch should be quoted with Five (5) Years of TAC Support and 5 years Hardware Warranty with advance hardware replacement.	
12.5	Bidder needs to submit bid specific MAF from the OEM.	
12.6	OEM should not share land border with India. OEM needs to share declaration on the letter head for the same	
12.7	OEM should be ISO 9001:2015 certified. Certificate to be enclosed	

12.8	OEM should have 7-8 RMA depots in India for faster replacements . Details to be shared on the OEM letter head.	
12.9	The switch should have MTBF of >800K Hours at 25° C	

24Port Non PoE Access Switch

24Port Non PoE Access Switch		
S No.	Specifications	Compliance (Yes/No)
1	Product details - Please specify	
1.1	Please mention Make, Model No. and Part Code.	
2	Architecture & Port Density	
2.1	Access Switch should provide 24 x 10/100/1G RJ45 Ports and 4x 1G/10G/25G SFP+ Slots, for Stacking/Uplinks, from Day 1.	
	Hardware, including modules, or Software, including licenses, to support all the speeds listed above, should be available from Day 1	
2.2	Should support Virtual Switching System (VSS) or Virtual Chassis (VC) or Virtual Switching Extension (VSX) or equivalent Switch Clustering/Stacking feature, where the Switch Clustering feature should combine multiple switches into a single network element. Switch should support aggregated stacking bandwidth of 800Gbps or more and 8 switches per stack or more.	
3	Performance	
3.1	Should provide Switch Fabric Bandwidth Capacity of 248 Gbps, or more.	
3.2	Should provide Packet Forwarding Capacity of 184 Mpps, or more.	
4	MAC Address and Route Table	
4.1	Should support up to 32K MAC addresses, or more.	
4.2	Should support 16K IPv4 routes and 4K IPv6 routes, or more.	
5	Physical Attributes	
5.1	Switch should be 1U and rack mountable in standard 19" rack.	
5.2	Should support 4GB RAM, 8GB Flash and 4MB Packet buffer or better	
6	Layer 2 features	

6.1	Should support Jumbo Frames (up to 9K bytes).	
6.2	Should support 4K Active VLANs, with the following features;	
	Port based VLANs	
	Dual-Mode VLANs	
	MAC-based VLANs	
	Dynamic VLAN Assignment	
	Dynamic MAC-based VLAN Activation	
	Dynamic Voice VLAN Assignment	
	VLAN mapping or VLAN Translation	
6.3	Should support Spanning Tree Protocols, with the following features;	
	802.1D Spanning Tree	
	802.1W Rapid Spanning Tree Protocol (RSTP)	
	802.1s Multiple Spanning Tree	
	802.1s Multiple Spanning Tree enhancement (MSTP+)	
	Fast Port Span, Fast Uplink Span or Equivalent	
	Compatibility with PVST/PVST+, PVRST+ and PVST+ or Equivalent	
	BPDU Guard	
	Root Guard for STP & MSTP	
	Port Loop Detection	
	Spanning Tree path cost method changes	
	MSTP path-cost configuration	
6.4	Should support Link Aggregation Groups (LAG), with the following features;	
	Static LAG	
	802.3ad Link Aggregation Control Protocol (Dynamic LAG)	
	Dynamic insertion and removal of ports	
	Support for LAG between different default port speeds	
6.5	Should support 802.1q Tunneling, with the following features;	

	802.1ad (Q-in-Q) tagging	
	Q-in-Q BPDU tunneling	
	Selective Q-in-Q	
6.6	Should support Private VLANs, with the following features.	
	PVLANs with dual mode support	
	PVLAN with LAG	
6.7	Should support VLAN Registration Protocol, with the following features;	
	Multiple VLAN Registration Protocol (MVRP)	
	MVRP with Per-VLAN STP and Per-VLAN RSTP	
6.8	Should support the following features;	
	Unicast Reverse Path Forwarding (uRPF)	
	Remote Fault Notification (RFN)	
	Link Fault Signaling (LFS)	
	Uni-Directional Link Detection (UDLD) on Tagged and Untagged Ports	
	To limit Unknown Unicast Packet Flooding (UUFB)	
	Virtual Extensible LAN (VXLAN)	
7	Layer 3 features	
7.1	Should support the following IPv4 and IPv6 Layer 3 Routing features;	
	Routing Between Directly Connected Subnets	
	Host routes & Virtual Interfaces	
	IPv4 & IPv6 Static Routes	
	RIP v1/v2 & RIPng	
	ECMP	
	OSPF v2, OSPF v3	
	PIM-SM, PIM-SSM, PIM-DM, PIM passive	
	Policy Based Routing (PBR)	
	VRRP v2 & VRRP v3	

	Non-Stop Routing (NSR)	
	GRE IP Tunnels	
	IPv6 over IPv4 tunnels and VRF	
	DHCP Server	
	MSDP	
8	Quality of Service (QoS) & Traffic Management	
8.1	Should support the following Quality of Service (QoS) features;	
	ACL Mapping and Marking of ToS/DSCP (CoS)	
	ACL Mapping and Marking of 802.1p	
	ACL Mapping to Priority Queue	
	Classifying and Limiting Flows Based on TCP Flags	
	DiffServ Support	
	Honoring DSCP and 802.1p (CoS)	
	Dynamic Buffer Allocation for QoS Priorities	
	Separate QoS Queuing for Unicast and Multicast	
	Priority Queue Management using Weighted Round Robin (WRR), Strict Priority (SP), and a combination of WRR and SP	
	Priority for PFC	
8.2	Should support the following Traffic Management features;	
	ACL-based Rate Limiting	
	Traffic Policies	
	Broadcast, Multicast, and Unknown Unicast Rate Limiting	
	Inbound Rate & Outbound Rate Limiting	
	CPU Rate Limiting	
9	Software Defined Networking (SDN)	
9.1	Should support the following SDN features and functionality;	
	OpenFlow v1.0 & v1.3	

	Hybrid Switch Mode	
	Hybrid Port Mode	
	Support for Multiple Controllers	
10	Security	
	Should support the following Security features;	
	Layer 3 & Layer 4 ACLs	
	Layer 2 ACLs (MAC)	
	DHCP Snooping	
	DHCP Client & Server	
	Dynamic ARP Inspection	
	Neighbor Discovery (ND) Inspection	
	Protection against Denial of Service (DoS) Attacks	
10.1	MAC Port Security	
	RADIUS/TACACS/TACACS+	
	Secure Copy (SCP)	
	Secure Shell (SSHv2)	
	Trusted Platform Module	
	Protected Ports	
	IP Source Guard (v4 & v6)	
	IPv6 RA Guard	
	RADSEC	
	The Switch should support the following Authentication features;	
	Authentication, Authorization, and Accounting (AAA)	
10.2	802.1X Authentication and Accounting	
	MAC Authentication and Accounting	
	Web Authentication	
	802.1x with Dynamic ACL Assignment	

	802.1x with Dynamic VLAN Assignment	
	802.1x and MAC Authentication on the same port	
	802.1x Authentication with IP Source Guard Protection	
	MAC Authentication with IP Source Guard Protection	
	MAC Authentication with Dynamic VLAN Assignment	
	MAC Authentication with Dynamic ACLs	
	MAC Authentication with 802.1x	
	802.1x together with Denial of Service (DoS) Attack Protection	
	Periodic Re-authentication for MAC Authentication	
	Periodic Re-authentication for 802.1x	
11	Monitoring & Manageability	
11.1	The Switch should support the following Monitoring & Management features;	
	RSPAN	
	NTP	
	LLDP & LLDP-MED	
	Cisco Discovery Protocol (CDP) for IPv4 and IPv6 Traffic or equivalent	
	Automation with Ansible & RESTCONF	
	DHCP Auto Configuration	
	SNMP v1, v2, and v3	
	Mirroring based on Port, IP ACL, MAC ACL and VLAN	
	Configuration Archive, Replace & Roll back	
	IP DHCP binding scalability of minimum 2K Devices	
11.2	Should support Integrated Standard based Command Line Interface (CLI), Telnet, TFTP, HTTP access to switch management/monitoring.	
11.3	Should support manageability using Network Management Software with Web based Graphical User Interface (GUI) and Cloud based Management Solutions.	
11.4	Should support NetFlow or sFlow or equivalent.	
12	Mandatory Compliance & Warranty and support:	

12.1	All switches, WiFi, WLC, Transceivers, AAA should be from the same OEM for better interoperatability, management and support	
12.2	The Switch OS should be EAL/NDPP and ROHS6 Certified. Certificate needs to be enclosed along with the bid	
12.3	The Switch must be MTCTE Certified and TEC certificate shall be submitted	
12.4	The Switch should be quoted with Five (5) Years of TAC Support and 5 years Hardware Warranty with advance hardware replacement.	
12.5	Bidder needs to submit bid specific MAF from the OEM.	
12.6	OEM should not share land border with India. OEM needs to share declaration on the letter head for the same	
12.7	OEM should be ISO 9001:2015 certified. Certificate to be enclosed	
12.8	OEM should have 7-8 RMA depots in India for faster replacements . Details to be shared on the OEM letter head.	
12.9	The switch should have MTBF of >800K Hours at 25° C	

48 Port POE Switch

48Port Gigabit PoE Access Switch		
Sl. No	Specifications	Compliance (Yes/No)
1	Product details - Please specify	
1.1	Please mention Make, Model No. and Part Code.	
2	Architecture & Port Density	
2.1	Access Switch should provide 48 x 10/100/1G PoE+ RJ45 Ports and with minimum 740 watts of PoE power budget and 4x 1G/10G/25G SFP+ Slots, for Stacking/Uplinks, from Day 1.	
	Hardware, including modules, or Software, including licenses, to support all the speeds listed above, should be available from Day 1	
2.2	Should support Virtual Switching System (VSS) or Virtual Chassis (VC) or Virtual Switching Extension (VSX) or equivalent Switch Clustering/Stacking feature, where the Switch Clustering feature should combine multiple switches into a single network element. Switch should support aggregated stacking bandwidth of 800Gbps or more and 8 switches per stack or more.	

3	Performance	
3.1	Should provide Switch Fabric Bandwidth Capacity of 296 Gbps, or more.	
3.2	Should provide Packet Forwarding Capacity of 220 Mpps, or more.	
4	MAC Address and Route Table	
4.1	Should support up to 32K MAC addresses, or more.	
4.2	Should support 16K IPv4 routes and 4K IPv6 routes, or more.	
5	Physical Attributes	
5.1	Switch should be 1U and rack mountable in standard 19" rack.	
5.2	Should support 4GB RAM, 8GB Flash and 4MB Packet buffer or better	
6	Layer 2 features	
6.1	Should support Jumbo Frames (up to 9K bytes).	
6.2	Should support 4K Active VLANs, with the following features;	
	Port based VLANs	
	Dual-Mode VLANs	
	MAC-based VLANs	
	Dynamic VLAN Assignment	
	Dynamic MAC-based VLAN Activation	
	Dynamic Voice VLAN Assignment	
	VLAN mapping or VLAN Translation	
6.3	Should support Spanning Tree Protocols, with the following features;	
	802.1D Spanning Tree	
	802.1W Rapid Spanning Tree Protocol (RSTP)	
	802.1s Multiple Spanning Tree	
	802.1s Multiple Spanning Tree enhancement (MSTP+)	
	Fast Port Span, Fast Uplink Span or Equivalent	
	Compatibility with PVST/PVST+, PVRST+ and PVST+ or Equivalent	
	BPDU Guard	

	Root Guard for STP & MSTP	
	Port Loop Detection	
	Spanning Tree path cost method changes	
	MSTP path-cost configuration	
6.4	Should support Link Aggregation Groups (LAG), with the following features;	
	Static LAG	
	802.3ad Link Aggregation Control Protocol (Dynamic LAG)	
	Dynamic insertion and removal of ports	
	Support for LAG between different default port speeds	
6.5	Should support 802.1q Tunneling, with the following features;	
	802.1ad (Q-in-Q) tagging	
	Q-in-Q BPDU tunneling	
	Selective Q-in-Q	
6.6	Should support Private VLANs, with the following features.	
	PVLANs with dual mode support	
	PVLAN with LAG	
6.7	Should support VLAN Registration Protocol, with the following features;	
	Multiple VLAN Registration Protocol (MVRP)	
	MVRP with Per-VLAN STP and Per-VLAN RSTP	
6.8	Should support the following features;	
	Unicast Reverse Path Forwarding (uRPF)	
	Remote Fault Notification (RFN)	
	Link Fault Signaling (LFS)	
	Uni-Directional Link Detection (UDLD) on Tagged and Untagged Ports	
	To limit Unknown Unicast Packet Flooding (UUFB)	
	Virtual Extensible LAN (VXLAN)	
7	Layer 3 features	

7.1	Should support the following IPv4 and IPv6 Layer 3 Routing features;	
	Routing Between Directly Connected Subnets	
	Host routes & Virtual Interfaces	
	IPv4 & IPv6 Static Routes	
	RIP v1/v2 & RIPng	
	ECMP	
	OSPF v2, OSPF v3	
	PIM-SM, PIM-SSM, PIM-DM, PIM passive	
	Policy Based Routing (PBR)	
	VRRP v2 & VRRP v3	
	Non-Stop Routing (NSR)	
	GRE IP Tunnels	
	IPv6 over IPv4 tunnels and VRF	
	DHCP Server	
	MSDP	
8	Quality of Service (QoS) & Traffic Management	
8.1	Should support the following Quality of Service (QoS) features;	
	ACL Mapping and Marking of ToS/DSCP (CoS)	
	ACL Mapping and Marking of 802.1p	
	ACL Mapping to Priority Queue	
	Classifying and Limiting Flows Based on TCP Flags	
	DiffServ Support	
	Honoring DSCP and 802.1p (CoS)	
	Dynamic Buffer Allocation for QoS Priorities	
	Separate QoS Queuing for Unicast and Multicast	
	Priority Queue Management using Weighted Round Robin (WRR), Strict Priority (SP), and a combination of WRR and SP	

	Priority for PFC	
8.2	Should support the following Traffic Management features;	
	ACL-based Rate Limiting	
	Traffic Policies	
	Broadcast, Multicast, and Unknown Unicast Rate Limiting	
	Inbound Rate & Outbound Rate Limiting	
	CPU Rate Limiting	
9	Software Defined Networking (SDN)	
9.1	Should support the following SDN features and functionality;	
	OpenFlow v1.0 & v1.3	
	Hybrid Switch Mode	
	Hybrid Port Mode	
	Support for Multiple Controllers	
10	Security	
10.1	Should support the following Security features;	
	Layer 3 & Layer 4 ACLs	
	Layer 2 ACLs (MAC)	
	DHCP Snooping	
	DHCP Client & Server	
	Dynamic ARP Inspection	
	Neighbor Discovery (ND) Inspection	
	Protection against Denial of Service (DoS) Attacks	
	MAC Port Security	
	RADIUS/TACACS/TACACS+	
	Secure Copy (SCP)	
	Secure Shell (SSHv2)	
	Trusted Platform Module	

	Protected Ports	
	IP Source Guard (v4 & v6)	
	IPv6 RA Guard	
	RADSEC	
10.2	The Switch should support the following Authentication features;	
	Authentication, Authorization, and Accounting (AAA)	
	802.1X Authentication and Accounting	
	MAC Authentication and Accounting	
	Web Authentication	
	802.1x with Dynamic ACL Assignment	
	802.1x with Dynamic VLAN Assignment	
	802.1x and MAC Authentication on the same port	
	802.1x Authentication with IP Source Guard Protection	
	MAC Authentication with IP Source Guard Protection	
	MAC Authentication with Dynamic VLAN Assignment	
	MAC Authentication with Dynamic ACLs	
	MAC Authentication with 802.1x	
	802.1x together with Denial of Service (DoS) Attack Protection	
	Periodic Reauthentication for MAC Authentication	
	Periodic Reauthentication for 802.1x	
11	Monitoring & Manageability	
11.1	The Switch should support the following Monitoring & Management features;	
	RSPAN	
	NTP	
	LLDP & LLDP-MED	
	Cisco Discovery Protocol (CDP) for IPv4 and IPv6 Traffic or equivalent	
	Automation with Ansible & RESTCONF	

	DHCP Auto Configuration	
	SNMP v1, v2, and v3	
	Mirroring based on Port, IP ACL, MAC ACL and VLAN	
	Configuration Archive, Replace & Roll back	
	IP DHCP binding scalability of minimum 2K Devices	
11.2	Should support Integrated Standard based Command Line Interface (CLI), Telnet, TFTP, HTTP access to switch management/monitoring.	
11.3	Should support manageability using Network Management Software with Web based Graphical User Interface (GUI) and Cloud based Management Solutions.	
11.4	Should support NetFlow or sFlow or equivalent.	
12	Mandatory Compliance & Warranty and support:	
12.1	All switches, WiFi, WLC, Transceivers, AAA should be from the same OEM for better interoperatability, management and support	
12.2	The Switch OS should be EAL/NDPP and ROHS6 Certified. Certificate needs to be enclosed along with the bid	
12.3	The Switch must be MTCTE Certified and TEC certificate shall be submitted	
12.4	The Switch should be quoted with Five (5) Years of TAC Support and 5 years Hardware Warranty with advance hardware replacement.	
12.5	Bidder needs to submit bid specific MAF from the OEM.	
12.6	OEM should not share land border with India. OEM needs to share declaration on the letter head for the same	
12.7	OEM should be ISO 9001:2015 certified. Certificate to be enclosed	
12.8	OEM should have 7-8 RMA depots in India for faster replacements . Details to be shared on the OEM letter head.	
12.9	The switch should have MTBF of >800K Hours at 25° C	

24 Port POE Switch

24Port Gigabit PoE Access Switch		
Sl. No	Specifications	Compliance (Yes/No)

1	Product details - Please specify	
1.1	Please mention Make, Model No. and Part Code.	
2	Architecture & Port Density	
2.1	Access Switch should provide 24 x 10/100/1G PoE+ RJ45 Ports and with minimum 370 watts of PoE power budget and 4x 1G/10G/25G SFP+ Slots, for Stacking/Uplinks, from Day 1.	
	Hardware, including modules, or Software, including licenses, to support all the speeds listed above, should be available from Day 1	
2.2	Should support Virtual Switching System (VSS) or Virtual Chassis (VC) or Virtual Switching Extension (VSX) or equivalent Switch Clustering/Stacking feature, where the Switch Clustering feature should combine multiple switches into a single network element. Switch should support aggregated stacking bandwidth of 800Gbps or more and 8 switches per stack or more.	
3	Performance	
3.1	Should provide Switch Fabric Bandwidth Capacity of 248 Gbps, or more.	
3.2	Should provide Packet Forwarding Capacity of 184 Mpps, or more.	
4	MAC Address and Route Table	
4.1	Should support up to 32K MAC addresses, or more.	
4.2	Should support 16K IPv4 routes and 4K IPv6 routes, or more.	
5	Physical Attributes	
5.1	Switch should be 1U and rack mountable in standard 19" rack.	
5.2	Should support 4GB RAM, 8GB Flash and 4MB Packet buffer or better	
6	Layer 2 features	
6.1	Should support Jumbo Frames (up to 9K bytes).	
6.2	Should support 4K Active VLANs, with the following features;	
	Port based VLANs	
	Dual-Mode VLANs	
	MAC-based VLANs	
	Dynamic VLAN Assignment	
	Dynamic MAC-based VLAN Activation	

	Dynamic Voice VLAN Assignment	
	VLAN mapping or VLAN Translation	
6.3	Should support Spanning Tree Protocols, with the following features;	
	802.1D Spanning Tree	
	802.1W Rapid Spanning Tree Protocol (RSTP)	
	802.1s Multiple Spanning Tree	
	802.1s Multiple Spanning Tree enhancement (MSTP+)	
	Fast Port Span, Fast Uplink Span or Equivalent	
	Compatibility with PVST/PVST+, PVRST+ and PVST+ or Equivalent	
	BPDU Guard	
	Root Guard for STP & MSTP	
	Port Loop Detection	
	Spanning Tree path cost method changes	
	MSTP path-cost configuration	
6.4	Should support Link Aggregation Groups (LAG), with the following features;	
	Static LAG	
	802.3ad Link Aggregation Control Protocol (Dynamic LAG)	
	Dynamic insertion and removal of ports	
	Support for LAG between different default port speeds	
6.5	Should support 802.1q Tunneling, with the following features;	
	802.1ad (Q-in-Q) tagging	
	Q-in-Q BPDU tunneling	
	Selective Q-in-Q	
6.6	Should support Private VLANs, with the following features.	
	PVLANs with dual mode support	
	PVLAN with LAG	
6.7	Should support VLAN Registration Protocol, with the following features;	

	Multiple VLAN Registration Protocol (MVRP)	
	MVRP with Per-VLAN STP and Per-VLAN RSTP	
	Should support the following features;	
	Unicast Reverse Path Forwarding (uRPF)	
	Remote Fault Notification (RFN)	
6.8	Link Fault Signaling (LFS)	
	Uni-Directional Link Detection (UDLD) on Tagged and Untagged Ports	
	To limit Unknown Unicast Packet Flooding (UUFB)	
	Virtual Extensible LAN (VXLAN)	
7	Layer 3 features	
	Should support the following IPv4 and IPv6 Layer 3 Routing features;	
	Routing Between Directly Connected Subnets	
	Host routes & Virtual Interfaces	
	IPv4 & IPv6 Static Routes	
	RIP v1/v2 & RIPng	
	ECMP	
	OSPF v2, OSPF v3	
7.1	PIM-SM, PIM-SSM, PIM-DM, PIM passive	
	Policy Based Routing (PBR)	
	VRRP v2 & VRRP v3	
	Non-Stop Routing (NSR)	
	GRE IP Tunnels	
	IPv6 over IPv4 tunnels and VRF	
	DHCP Server	
	MSDP	
8	Quality of Service (QoS) & Traffic Management	
8.1	Should support the following Quality of Service (QoS) features;	

	ACL Mapping and Marking of ToS/DSCP (CoS)	
	ACL Mapping and Marking of 802.1p	
	ACL Mapping to Priority Queue	
	Classifying and Limiting Flows Based on TCP Flags	
	DiffServ Support	
	Honoring DSCP and 802.1p (CoS)	
	Dynamic Buffer Allocation for QoS Priorities	
	Separate QoS Queuing for Unicast and Multicast	
	Priority Queue Management using Weighted Round Robin (WRR), Strict Priority (SP), and a combination of WRR and SP	
	Priority for PFC	
8.2	Should support the following Traffic Management features;	
	ACL-based Rate Limiting	
	Traffic Policies	
	Broadcast, Multicast, and Unknown Unicast Rate Limiting	
	Inbound Rate & Outbound Rate Limiting	
	CPU Rate Limiting	
9	Software Defined Networking (SDN)	
9.1	Should support the following SDN features and functionality;	
	OpenFlow v1.0 & v1.3	
	Hybrid Switch Mode	
	Hybrid Port Mode	
	Support for Multiple Controllers	
10	Security	
10.1	Should support the following Security features;	
	Layer 3 & Layer 4 ACLs	
	Layer 2 ACLs (MAC)	

	DHCP Snooping	
	DHCP Client & Server	
	Dynamic ARP Inspection	
	Neighbor Discovery (ND) Inspection	
	Protection against Denial of Service (DoS) Attacks	
	MAC Port Security	
	RADIUS/TACACS/TACACS+	
	Secure Copy (SCP)	
	Secure Shell (SSHv2)	
	Trusted Platform Module	
	Protected Ports	
	IP Source Guard (v4 & v6)	
	IPv6 RA Guard	
	RADSEC	
10.2	The Switch should support the following Authentication features;	
	Authentication, Authorization, and Accounting (AAA)	
	802.1X Authentication and Accounting	
	MAC Authentication and Accounting	
	Web Authentication	
	802.1x with Dynamic ACL Assignment	
	802.1x with Dynamic VLAN Assignment	
	802.1x and MAC Authentication on the same port	
	802.1x Authentication with IP Source Guard Protection	
	MAC Authentication with IP Source Guard Protection	
	MAC Authentication with Dynamic VLAN Assignment	
	MAC Authentication with Dynamic ACLs	
	MAC Authentication with 802.1x	

	802.1x together with Denial of Service (DoS) Attack Protection	
	Periodic Reauthentication for MAC Authentication	
	Periodic Reauthentication for 802.1x	
11	Monitoring & Manageability	
11.1	The Switch should support the following Monitoring & Management features;	
	RSPAN	
	NTP	
	LLDP & LLDP-MED	
	Cisco Discovery Protocol (CDP) for IPv4 and IPv6 Traffic or equivalent	
	Automation with Ansible & RESTCONF	
	DHCP Auto Configuration	
	SNMP v1, v2, and v3	
	Mirroring based on Port, IP ACL, MAC ACL and VLAN	
	Configuration Archive, Replace & Roll back	
	IP DHCP binding scalability of minimum 2K Devices	
11.2	Should support Integrated Standard based Command Line Interface (CLI), Telnet, TFTP, HTTP access to switch management/monitoring.	
11.3	Should support manageability using Network Management Software with Web based Graphical User Interface (GUI) and Cloud based Management Solutions.	
11.4	Should support NetFlow or sFlow or equivalent.	
12	Mandatory Compliance & Warranty and support:	
12.1	Should support Virtual Switching System (VSS) or Virtual Chassis (VC) or Virtual Switching Extension (VSX) or equivalent Switch Clustering/Stacking feature, where the Switch Clustering feature should combine multiple switches into a single network element. Switch should support aggregated stacking bandwidth of 800Gbps or more and 8 switches per stack or more.	
12.2	The Switch OS should be EAL/NDPP and ROHS6 Certified. Certificate needs to be enclosed along with the bid	
12.3	The Switch must be MTCTE Certified and TEC certificate shall be submitted	
12.4	The Switch should be quoted with Five (5) Years of TAC Support and 5 years	

	Hardware Warranty with advance hardware replacement.	
12.5	Bidder needs to submit bid specific MAF from the OEM.	
12.6	OEM should not share land border with India. OEM needs to share declaration on the letter head for the same	
12.7	OEM should be ISO 9001:2015 certified. Certificate to be enclosed	
12.8	OEM should have 7-8 RMA depots in India for faster replacements . Details to be shared on the OEM letter head.	
12.9	The switch should have MTBF of >800K Hours at 25° C	

24Port Multigigabit PoE Access Switch

24Port Multigigabit PoE Access Switch		
Sl. No	Specifications	Compliance (Yes/No)
1	Product details - Please specify	
1.1	Please mention Make, Model No. and Part Code.	
2	Architecture & Port Density	
2.1	Access Switch should provide 24 x 10/100/1G/2.5Gbps PoE+ RJ45 Ports and with minimum 740 watts of PoE power budget and 4x 1G/10G/25G SFP+ Slots, for Stacking/Uplinks, from Day 1.	
	Hardware, including modules, or Software, including licenses, to support all the speeds listed above, should be available from Day 1	
2.2	Should support Virtual Switching System (VSS) or Virtual Chassis (VC) or Virtual Switching Extension (VSX) or equivalent Switch Clustering/Stacking feature, where the Switch Clustering feature should combine multiple switches into a single network element. Switch should support aggregated stacking bandwidth of 800Gbps or more and 8 switches per stack or more.	
3	Performance	
3.1	Should provide Switch Fabric Bandwidth Capacity of 320 Gbps, or more.	
3.2	Should provide Packet Forwarding Capacity of 237 Mpps, or more.	
4	MAC Address and Route Table	
4.1	Should support up to 32K MAC addresses, or more.	

4.2	Should support 16K IPv4 routes and 4K IPv6 routes, or more.	
5	Physical Attributes	
5.1	Switch should be 1U and rack mountable in standard 19" rack.	
5.2	Should support 4GB RAM, 8GB Flash and 4MB Packet buffer or better	
6	Layer 2 features	
6.1	Should support Jumbo Frames (up to 9K bytes).	
6.2	Should support 4K Active VLANs, with the following features;	
	Port based VLANs	
	Dual-Mode VLANs	
	MAC-based VLANs	
	Dynamic VLAN Assignment	
	Dynamic MAC-based VLAN Activation	
	Dynamic Voice VLAN Assignment	
	VLAN mapping or VLAN Translation	
6.3	Should support Spanning Tree Protocols, with the following features;	
	802.1D Spanning Tree	
	802.1W Rapid Spanning Tree Protocol (RSTP)	
	802.1s Multiple Spanning Tree	
	802.1s Multiple Spanning Tree enhancement (MSTP+)	
	Fast Port Span, Fast Uplink Span or Equivalent	
	Compatibility with PVST/PVST+, PVRST+ and PVST+ or Equivalent	
	BPDU Guard	
	Root Guard for STP & MSTP	
	Port Loop Detection	
	Spanning Tree path cost method changes	
	MSTP path-cost configuration	
6.4	Should support Link Aggregation Groups (LAG), with the following features;	

	Static LAG	
	802.3ad Link Aggregation Control Protocol (Dynamic LAG)	
	Dynamic insertion and removal of ports	
	Support for LAG between different default port speeds	
6.5	Should support 802.1q Tunneling, with the following features;	
	802.1ad (Q-in-Q) tagging	
	Q-in-Q BPDU tunneling	
	Selective Q-in-Q	
6.6	Should support Private VLANs, with the following features.	
	PVLANs with dual mode support	
	PVLAN with LAG	
6.7	Should support VLAN Registration Protocol, with the following features;	
	Multiple VLAN Registration Protocol (MVRP)	
	MVRP with Per-VLAN STP and Per-VLAN RSTP	
6.8	Should support the following features;	
	Unicast Reverse Path Forwarding (uRPF)	
	Remote Fault Notification (RFN)	
	Link Fault Signaling (LFS)	
	Uni-Directional Link Detection (UDLD) on Tagged and Untagged Ports	
	To limit Unknown Unicast Packet Flooding (UUFB)	
	Virtual Extensible LAN (VXLAN)	
7	Layer 3 features	
7.1	Should support the following IPv4 and IPv6 Layer 3 Routing features;	
	Routing Between Directly Connected Subnets	
	Host routes & Virtual Interfaces	
	IPv4 & IPv6 Static Routes	
	RIP v1/v2 & RIPng	

	ECMP	
	OSPF v2, OSPF v3	
	PIM-SM, PIM-SSM, PIM-DM, PIM passive	
	Policy Based Routing (PBR)	
	VRRP v2 & VRRP v3	
	Non-Stop Routing (NSR)	
	GRE IP Tunnels	
	IPv6 over IPv4 tunnels and VRF	
	DHCP Server	
	MSDP	
8	Quality of Service (QoS) & Traffic Management	
8.1	Should support the following Quality of Service (QoS) features;	
	ACL Mapping and Marking of ToS/DSCP (CoS)	
	ACL Mapping and Marking of 802.1p	
	ACL Mapping to Priority Queue	
	Classifying and Limiting Flows Based on TCP Flags	
	DiffServ Support	
	Honoring DSCP and 802.1p (CoS)	
	Dynamic Buffer Allocation for QoS Priorities	
	Separate QoS Queuing for Unicast and Multicast	
	Priority Queue Management using Weighted Round Robin (WRR), Strict Priority (SP), and a combination of WRR and SP	
	Priority for PFC	
8.2	Should support the following Traffic Management features;	
	ACL-based Rate Limiting	
	Traffic Policies	
	Broadcast, Multicast, and Unknown Unicast Rate Limiting	

	Inbound Rate & Outbound Rate Limiting	
	CPU Rate Limiting	
9	Software Defined Networking (SDN)	
	Should support the following SDN features and functionality;	
	OpenFlow v1.0 & v1.3	
9.1	Hybrid Switch Mode	
	Hybrid Port Mode	
	Support for Multiple Controllers	
10	Security	
	Should support the following Security features;	
	Layer 3 & Layer 4 ACLs	
	Layer 2 ACLs (MAC)	
	DHCP Snooping	
	DHCP Client & Server	
	Dynamic ARP Inspection	
	Neighbor Discovery (ND) Inspection	
	Protection against Denial of Service (DoS) Attacks	
10.1	MAC Port Security	
	RADIUS/TACACS/TACACS+	
	Secure Copy (SCP)	
	Secure Shell (SSHv2)	
	Trusted Platform Module	
	Protected Ports	
	IP Source Guard (v4 & v6)	
	IPv6 RA Guard	
	RADSEC	
10.2	The Switch should support the following Authentication features;	

	Authentication, Authorization, and Accounting (AAA)	
	802.1X Authentication and Accounting	
	MAC Authentication and Accounting	
	Web Authentication	
	802.1x with Dynamic ACL Assignment	
	802.1x with Dynamic VLAN Assignment	
	802.1x and MAC Authentication on the same port	
	802.1x Authentication with IP Source Guard Protection	
	MAC Authentication with IP Source Guard Protection	
	MAC Authentication with Dynamic VLAN Assignment	
	MAC Authentication with Dynamic ACLs	
	MAC Authentication with 802.1x	
	802.1x together with Denial of Service (DoS) Attack Protection	
	Periodic Reauthentication for MAC Authentication	
	Periodic Reauthentication for 802.1x	
11	Monitoring & Manageability	
11.1	The Switch should support the following Monitoring & Management features;	
	RSPAN	
	NTP	
	LLDP & LLDP-MED	
	Cisco Discovery Protocol (CDP) for IPv4 and IPv6 Traffic or equivalent	
	Automation with Ansible & RESTCONF	
	DHCP Auto Configuration	
	SNMP v1, v2, and v3	
	Mirroring based on Port, IP ACL, MAC ACL and VLAN	
	Configuration Archive, Replace & Roll back	
	IP DHCP binding scalability of minimum 2K Devices	

11.2	Should support Integrated Standard based Command Line Interface (CLI), Telnet, TFTP, HTTP access to switch management/monitoring.	
11.3	Should support manageability using Network Management Software with Web based Graphical User Interface (GUI) and Cloud based Management Solutions.	
11.4	Should support NetFlow or sFlow or equivalent.	
12	Mandatory Compliance & Warranty and support:	
12.1	All switches, WiFi, WLC, Transceivers, AAA should be from the same OEM for better interoperatability, management and support	
12.2	The Switch OS should be EAL/NDPP and ROHS6 Certified. Certificate needs to be enclosed along with the bid	
12.3	The Switch must be MTCTE Certified and TEC certificate shall be submitted	
12.4	The Switch should be quoted with Five (5) Years of TAC Support and 5 years Hardware Warranty with advance hardware replacement.	
12.5	Bidder needs to submit bid specific MAF from the OEM.	
12.6	OEM should not share land border with India. OEM needs to share declaration on the letter head for the same	
12.7	OEM should be ISO 9001:2015 certified. Certificate to be enclosed	
12.8	OEM should have 7-8 RMA depots in India for faster replacements . Details to be shared on the OEM letter head.	
12.9	The switch should have MTBF of >500K Hours at 25° C	

8 Port Multigigabit PoE Access Switch

8Port Multigigabit PoE Access Switch		
Sl. No	Specifications	Compliance (Yes/No)
1	Product details - Please specify	
1.1	Please mention Make, Model No. and Part Code.	
2	Architecture & Port Density	
2.1	Access Switch should provide 4 x 100/1G/2.5Gbps PoE+ RJ45 Ports, 4 x 100/1/2.5/5/10Gbps and 2 x 1/10/25Gbps SFP28 ports for for Stacking/Uplinks.	

	Switch should have minimum 240 watts of PoE power budget from Day 1.	
	Hardware, including modules, or Software, including licenses, to support all the speeds listed above, should be available from Day 1	
2.2	Should support Virtual Switching System (VSS) or Virtual Chassis (VC) or Virtual Switching Extension (VSX) or equivalent Switch Clustering/Stacking feature, where the Switch Clustering feature should combine multiple switches into a single network element. Switch should support stacking of 8 switches per stack or more.	
3	Performance	
3.1	Should provide Switch Fabric Bandwidth Capacity of 200 Gbps, or more.	
3.2	Should provide Packet Forwarding Capacity of 148 Mpps, or more.	
4	MAC Address and Route Table	
4.1	Should support up to 32K MAC addresses, or more.	
4.2	Should support 16K IPv4 routes and 4K IPv6 routes, or more.	
5	Physical Attributes	
5.1	Switch should be 1U and rack mountable in standard 19" rack.	
5.2	Should support 4GB RAM, 8GB Flash and 4MB Packet buffer or better	
6	Layer 2 features	
6.1	Should support Jumbo Frames (up to 9K bytes).	
6.2	Should support 4K Active VLANs, with the following features;	
	Port based VLANs	
	Dual-Mode VLANs	
	MAC-based VLANs	
	Dynamic VLAN Assignment	
	Dynamic MAC-based VLAN Activation	
	Dynamic Voice VLAN Assignment	
	VLAN mapping or VLAN Translation	
6.3	Should support Spanning Tree Protocols, with the following features;	

	802.1D Spanning Tree	
	802.1W Rapid Spanning Tree Protocol (RSTP)	
	802.1s Multiple Spanning Tree	
	802.1s Multiple Spanning Tree enhancement (MSTP+)	
	Fast Port Span, Fast Uplink Span or Equivalent	
	Compatibility with PVST/PVST+, PVRST+ and PVST+ or Equivalent	
	BPDU Guard	
	Root Guard for STP & MSTP	
	Port Loop Detection	
	Spanning Tree path cost method changes	
	MSTP path-cost configuration	
6.4	Should support Link Aggregation Groups (LAG), with the following features;	
	Static LAG	
	802.3ad Link Aggregation Control Protocol (Dynamic LAG)	
	Dynamic insertion and removal of ports	
	Support for LAG between different default port speeds	
6.5	Should support 802.1q Tunneling, with the following features;	
	802.1ad (Q-in-Q) tagging	
	Q-in-Q BPDU tunneling	
	Selective Q-in-Q	
6.6	Should support Private VLANs, with the following features.	
	PVLANs with dual mode support	
	PVLAN with LAG	
6.7	Should support VLAN Registration Protocol, with the following features;	
	Multiple VLAN Registration Protocol (MVRP)	
	MVRP with Per-VLAN STP and Per-VLAN RSTP	
6.8	Should support the following features;	

	Unicast Reverse Path Forwarding (uRPF)	
	Remote Fault Notification (RFN)	
	Link Fault Signaling (LFS)	
	Uni-Directional Link Detection (UDLD) on Tagged and Untagged Ports	
	To limit Unknown Unicast Packet Flooding (UUFB)	
	Virtual Extensible LAN (VXLAN)	
7	Layer 3 features	
7.1	Should support the following IPv4 and IPv6 Layer 3 Routing features;	
	Routing Between Directly Connected Subnets	
	Host routes & Virtual Interfaces	
	IPv4 & IPv6 Static Routes	
	RIP v1/v2 & RIPng	
	ECMP	
	OSPF v2, OSPF v3	
	PIM-SM, PIM-SSM, PIM-DM, PIM passive	
	Policy Based Routing (PBR)	
	VRRP v2 & VRRP v3	
	Non-Stop Routing (NSR)	
	GRE IP Tunnels	
	IPv6 over IPv4 tunnels and VRF	
	DHCP Server	
	MSDP	
8	Quality of Service (QoS) & Traffic Management	
8.1	Should support the following Quality of Service (QoS) features;	
	ACL Mapping and Marking of ToS/DSCP (CoS)	
	ACL Mapping and Marking of 802.1p	
	ACL Mapping to Priority Queue	

	Classifying and Limiting Flows Based on TCP Flags	
	DiffServ Support	
	Honoring DSCP and 802.1p (CoS)	
	Dynamic Buffer Allocation for QoS Priorities	
	Separate QoS Queuing for Unicast and Multicast	
	Priority Queue Management using Weighted Round Robin (WRR), Strict Priority (SP), and a combination of WRR and SP	
	Priority for PFC	
8.2	Should support the following Traffic Management features;	
	ACL-based Rate Limiting	
	Traffic Policies	
	Broadcast, Multicast, and Unknown Unicast Rate Limiting	
	Inbound Rate & Outbound Rate Limiting	
	CPU Rate Limiting	
9	Software Defined Networking (SDN)	
9.1	Should support the following SDN features and functionality;	
	OpenFlow v1.0 & v1.3	
	Hybrid Switch Mode	
	Hybrid Port Mode	
	Support for Multiple Controllers	
10	Security	
10.1	Should support the following Security features;	
	Layer 3 & Layer 4 ACLs	
	Layer 2 ACLs (MAC)	
	DHCP Snooping	
	DHCP Client & Server	
	Dynamic ARP Inspection	

	Neighbor Discovery (ND) Inspection	
	Protection against Denial of Service (DoS) Attacks	
	MAC Port Security	
	RADIUS/TACACS/TACACS+	
	Secure Copy (SCP)	
	Secure Shell (SSHv2)	
	Trusted Platform Module	
	Protected Ports	
	IP Source Guard (v4 & v6)	
	IPv6 RA Guard	
	RADSEC	
10.2	The Switch should support the following Authentication features;	
	Authentication, Authorization, and Accounting (AAA)	
	802.1X Authentication and Accounting	
	MAC Authentication and Accounting	
	Web Authentication	
	802.1x with Dynamic ACL Assignment	
	802.1x with Dynamic VLAN Assignment	
	802.1x and MAC Authentication on the same port	
	802.1x Authentication with IP Source Guard Protection	
	MAC Authentication with IP Source Guard Protection	
	MAC Authentication with Dynamic VLAN Assignment	
	MAC Authentication with Dynamic ACLs	
	MAC Authentication with 802.1x	
	802.1x together with Denial of Service (DoS) Attack Protection	
	Periodic Reauthentication for MAC Authentication	
	Periodic Reauthentication for 802.1x	

10.3	The Switch should support Cisco ISE/Aruba ClearPass/other Authentication solutions	
11	Monitoring & Manageability	
11.1	The Switch should support the following Monitoring & Management features;	
	RSPAN	
	NTP	
	LLDP & LLDP-MED	
	Cisco Discovery Protocol (CDP) for IPv4 and IPv6 Traffic or equivalent	
	Automation with Ansible & RESTCONF	
	DHCP Auto Configuration	
	SNMP v1, v2, and v3	
	Mirroring based on Port, IP ACL, MAC ACL and VLAN	
	Configuration Archive, Replace & Roll back	
	IP DHCP binding scalability of minimum 2K Devices	
11.2	Should support Integrated Standard based Command Line Interface (CLI), Telnet, TFTP, HTTP access to switch management/monitoring.	
11.3	Should support manageability using Network Management Software with Web based Graphical User Interface (GUI) and Cloud based Management Solutions.	
11.4	Should support NetFlow or sFlow or equivalent.	
12	Mandatory Compliance & Warranty and support:	
12.1	All switches, WiFi, WLC, Transceivers, AAA should be from the same OEM for better interoperatability, management and support	
12.2	The Switch OS should be EAL/NDPP and ROHS6 Certified. Certificate needs to be enclosed along with the bid	
12.3	The Switch must be MTCTE Certified and TEC certificate shall be submitted	
12.4	The Switch should be quoted with Five (5) Years of TAC Support and 5 years Hardware Warranty with advance hardware replacement.	
12.5	Bidder needs to submit bid specific MAF from the OEM.	
12.6	OEM should not share land border with India. OEM needs to share declaration on the letter head for the same	

12.7	OEM should be ISO 9001:2015 certified. Certificate to be enclosed	
12.8	OEM should have 7-8 RMA depots in India for faster replacements . Details to be shared on the OEM letter head.	
12.9	The switch should have MTBF of >500K Hours at 25° C	

Fiber SFP Module

10G SFP+ SR Optics (300 Meters)		
SN	Specifications	Compliance (Yes/No)
1	SFP should support Multi-Mode Fiber 850nm.	
2	SFP should support OM3 Multi-Mode Fiber Cable	
3	SFP should be 802.3ae compliant and shall support a distanc up to 300 Meters	
4	SFP should have LC Connector	
5	SFP should be protocol independent & Hot-Swappable	
6	SFP should be MSA, ROHS 5 & 6 Compliant	
7	SFP should support Digital Optical Monitoring	
8	SFP should support operating temperature from (00 C to 700C)	

10G SFP+ LR Optics (10 KM)		
SN	Specifications	Compliance (Yes/No)
1	SFP should support Single-Mode Fiber 1310nm.	
2	SFP should support Single-Mode Fiber Cable	
3	SFP should be 802.3ae compliant and shall support a distanc up to 10 Kilometers	
4	SFP should have LC Connector	
5	SFP should be protocol independent & Hot-Swappable	
6	SFP should be MSA, ROHS 5 & 6 Compliant	

7	SFP should support Digital Optical Monitoring	
8	SFP should support operating temperature from (00 C to 700C)	

Wireless Controller

Wireless Controller		
S. No	Specification	Compliance (Yes/No)
1	Wireless Controller should be tested for EAL 2/NDPP or above under Common Criteria Certification . Certificate must be submitted.	
2	Wireless Controller should be MTCTE (Mandatory Testing & Certification Of Telecommunication Equipment) Certified and Certificate issued by TEC (Telecommunication Engineering Center), Department of Telecommunications must be submitted.	
3	Wireless Controller should be quoted with 05 years of TAC Support & 5 years Hardware Warranty with advance hardware replacement	
4	Wireless Controller should support operating temperature from 00 to 400 degree celsius.	
5	Wireless Controller should have minimum of 4 x 1Gigabit Ethernet & 4 x 10Gigabit Ports or more. 4x10G Multimode SFP+ transceivers to be supplied with the controller	
6	Wireless Controller should support 1+1 Internal Redundant Power Supply.	
7	Controller should be able to manage the required number of APs on a single appliance from day one and should be scalable up to 2000 AP on single appliance and 6000 AP in a clustered configuration.Cloud Based solution will not be accepted. The controller or the solution should be able to monitor and manage the required number of switches.	
8	Support for N:1 redundancy for controller. In case primary controller goes down all features should be supported by redundant controller. Software/ Cloud Based Controller Solution will not be accepted.	
9	Each Controller or its cluster should have capacity to handle 40,000 or more Concurrent devices.	
10	Redundancy Features: WLC must support Active: Active with N+1 redundancy.	
11	Controller should support minimum 2000 WLAN’s.	

12	The proposed WLAN solution must support a distributed forwarding/local breakout architecture in which only client authentication is tunneled to the centralized controller; all client data traffic is forwarded directly on towards its destination via the clients default gateway. Further: a.Specify any loss of functionality, caveats or loss of capacity/performance is exhibited by the solution in this distributed forwarding mode. b.On a per WLAN (SSID) basis there must be an option to tunnel traffic to the controller either unencrypted or encrypted format	
13	Controller should provide air-time fairness between the different speed clients – slower clients should not be starved by the faster clients and faster clients should not adversely affected by slower clients.	
14	Controller should have the Ability to map SSID to VLAN and dynamic VLAN support for same SSID.	
15	Controller should support automatic channel selection for interference avoidance.	
16	Controller should support external Captive Portal Integration - Web-services based API for external web-portals to integrate with the controller	
17	Controller should have the capability to limit/prevent clients from using static IP addresses thereby enhancing network efficiency and preventing network conflicts.	
18	The controller or WLAN solution should support client troubleshooting feature that allows an administrator to focus on a specific client device and its connectivity status. The tool should track the step-by-step progress of the client's connection, through 802.11 stages, RADIUS, EAP authentication, captive portal redirects, encryption key setup, DHCP, roaming, and more (depending on WLAN type).	
19	For troubleshooting purpose the administrator of the controller must have the ability to remotely capture 802.11 and/or 802.3 frames from an access point without disrupting client access.	
20	In order to have good visibility on the utilization of an AP, the controller or proposed solution should be able to provide the following statistics for each AP: a. List of all the SSIDs deployed on each of the radio of the AP. b. Number of client devices associated on each radio c. Average client RSSI. d.Data sent/received e. Air Time utilization (%RX, %TX, %Busy) f. Statistics on retransmitted packets g. Graphical collation of various trend and troubleshooting data such as estimated channel capacity, current channel utilization, number of associated clients, RF pollution, other APs detected	

21	The controller or proposed solution should support Role-based Access Controls that can provide policy controls on a single SSID such as: a.Time of day access b.VLAN assignment c.Per device rate limiting d.Deny/Allow specified device OS types	
22	The controller should support in built spectrum analysis feature.	
23	The controller should support the ability to create different zones in which AP can be grouped logically or physically based on location for example different buildings of a campus can be configured as different zones so that each zone will have different configuration and policies.	
24	The controller should support Hotspot 2.0 (pass point).	
25	Access points can discover controllers on the same L2 domain without requiring any configuration on the access point.	
26	Access points can discover controllers across Layer-3 network through DHCP or DNS option	
27	WIRELESS SECURITY & Authentication: Open, 802.1x/EAP, PSK, WISPr, WPA, WPA2-AES. Fast EAP-SIM re-authentication. EAP-SIM, EAP-AKA, EAP-AKA over WLAN for 802.1X Wi-Fi. It should also support WPA3 and Enhanced Open	
28	To aid to physically locating rogue devices in conjunction with scanning at the APs the controller should be able to list/classify detected Rogue Devices. Further: a) The information presented must include information about the detecting AP(s) and the rogues signal strength relative to them. It should display rogues on a map b)The controller should be able to send a filtered notification to the administrator when a rogue device has been detected c)Neighbouring APs should be capable of de-authenticating clients from a malicious rogue device i.e. one which is spoofing the BSSID or SSID of a genuine managed AP. d) The controller or proposed solution should support rogue classification policy. The policy should support rules for AdHoc Networks, Clear to Send (CTS) Abuse, De-Authentication Flood, Disassociation Flood, Request to Send (RTS) Abuse, Excessive Power, MAC (BSSID) Spoofing, Same Network, NULL SSID and SSID Spoofing. e)The WLAN or proposed solution should support Known, Ignore, Malicious and Rogue as part of WIPS classification types.	
29	WLC Should support L2 Client Isolation so User cannot access each other's devices. Isolation should have option to apply on AP or SSID's.	
30	Support for Walled Garden "Walled Garden" functionality to allow restricted access to select destinations by unauthorized wireless users.	
31	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.	
32	The controller should provide a captive portal to authenticate Guest users that are not part of the organization via a Guest pass key. Further the solution must provide:	
	a. Provide a web-based application that allows non-technical staff to create Guest passes that are valid for a time limited duration	
	b. Allow the IT Administrator to view and delete individual Guest passes	
	c. Allow for batch generation of Guest passes	
	d. Provide customizable Guest portal and guest pass instructions.	
33	The controller or overall solution must also support Self registration of Guests.	
34	The controller must be capable of identifying device host OS type and the host name. Further the solution must be able to utilise the host OS information to provide per WLAN policy based access such as allow/deny access, rate limit and assign to VLAN	
35	When Wireless Mesh is enabled, the controller should be able to show the mesh topology on floor plans in a graphical format.	
36	The Wireless Mesh should support self-healing whereby if Root AP goes down then the Mesh AP should be able to automatically find and connect to another Root AP	
37	WLC should be able to present a customizable dashboard with information on the status of the WLAN network.	
38	The WLAN solution should support import of floor plans for indoor AP.	
39	WLC 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.	
40	The controller or its integrated solution must support APIs for easier management and integration with existing network management devices. Provide the list of APIs supported.	
41	WLC or integrated solution should provide customized reporting of historical WLAN information.	
42	Controller should support Filtering of Alarms and event Log based on APs, SSID or Zones	
43	Controller should support Syslog support towards external syslog server	
44	Controller should support per SSID or dynamic Per user bandwidth Rate Limiting	
45	Controller should support Self-healing (on detection of RF interference or loss of RF coverage) and vendor should provide their Interference mitigation techniques.	

46	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.	
47	WLC shall support Quality of Service features like 802.11e based QoS enhancements, WMM or equivalent and U-APSD to provide best performance on Video applications.	
48	The controller should provide Application recognition to allow the administrator to gain insight on the applications in use and the bandwidth they consume per system and per user.	
49	The Controller or WLAN solution should support Wired network (Network Switch) & Wireless Access Point (Indoor & Outdoor) management from single management interface.	
50	The Controller or WLAN solution should support switch registration and authentication	
51	The Controller or WLAN solution should support Switch inventory (model, FW version, last backup, etc)	
52	The Controller or WLAN solution should support Health and performance monitoring (status, traffic stats, errors, clients etc) with alarms	
53	The Controller or WLAN solution should support switch Firmware Upgrade	
54	The Controller or WLAN solution should support Switch configuration file backup and restore	
55	The Controller or WLAN solution should support Client troubleshooting - search by Client MAC to find the AP/switch port for that client	
56	Bidder needs to submit bid specific MAF from the OEM.	
57	OEM End-of-sale declaration shall not have been released for the quoted model at the time of the bid submission.	
58	Wireless Controller shall conform to TEC EMI EMC Standard EN/IEC 60950-1, EN 55022, EN 61000-3-2, EN61000-3-3. TEC certificate shall be submitted	
59	Wireless Controller should be capable to integrate with Cloud Based Network Analystics Engine to provide Wireless Performance Insights, KPIs and what are the applications (Top N apps) that are consuming the most network bandwidth, monitors application traffic arriving from users (Top N talkers)	
60	All switches, WiFi, WLC, Transceivers, AAA should be from the same OEM for better interoperatability, management and support	

Indoor WiFi Access Point

WiFi6 Indoor WiFi Access Point		
S. No	Specification	Compliance (Yes/No)
	General Features	
1	Access Point should be tested for EAL 2/NDPP or above under Common Criteria Certification or Certificate issued by Indian Common Criteria Certification Scheme (IC3S) Certificate must be submitted.	
2	Access Point should be MTCTE (Mandatory Testing & Certification Of Telecommunication Equipment) Certified and Certificate issued by TEC (Telecommunication Engineering Center), Department of Telecommunications must be submitted.	
3	Access Point should have been approved by Wireless Planning Commission (TRAI, Govt. of India), ETA Certificate must be submitted.	
4	Access Point must be Wi-Fi Alliance Cetified to ensure the interoperatibility with othe make client deivces.	
5	Access Point should be quoted with 05 years of TAC Support & 5 years for Hardware Warranty .	
6	Access Point should support operating temperature from 00 to 500 degree celsius.	
	Radio Specifications	
7	Access Point should be dual-band, dual-radio indoor access point which should support six spatial streams 4x4:4 SU/MU-MIMO on 5GHz and 2x2:2 SU/MU-MIMO on 2.4GHz.	
8	Access Point should support IEEE 802.11 a/b/g/n/ac/ax standards.	
9	Access Point should support total data rates of 2974 Mbps (5Ghz: 2400Mbps & 2.4Ghz: 574 Mbps)	
10	Access Point should support Channelization at 20 Mhz, 40Mhz, 80 Mhz, 160/ 80+80Mhz	
11	Access Point should provide 26dBm transmit power on both radios as per TRAI-WPC Regulatory Norms. Access Point should have -96dBm or lower receive sensitivity.	
12	Access Point should have adaptive antenna technology for performance optimization and interference mitigiation features. Access Point should provide better coverage and performance utlizing multi-directional antenna patterns and polarization with maximal ratio combining.	
13	Access Point should direct the radio signals per-device on a packet-by-packet in real time to support high deivce density environments. Antenna should operate without the	

	need for device feedback to support devices using legacy standards.	
	Interface & Power Requirements	
14	Access Point PoE port should have 1 x 2.5Gbps PoE+ and 1 x 1Gbps Ethernet Port and 1 x USB Port	
	Networking Requirements	
15	Access Point should have capacity to handle minimum 500 concurrent devices.	
16	Access Point should support minimum 30 SSID or more.	
17	Access Point should have built-in/ external support for BLE and Zigbee for IoT integration	
18	Access Point should have built-in diagnostics tools such as Spectrum Analyzer to analyse the RF Channel for Interference & Client speed test etc.	
19	Access Point should support Airtime Fairness, Client Load Balancing, Airtime Based WLAN Prioritization.	
20	Access Point should be flexible harwdare to be deployed as Standalone, Controller less (Cluster), Controller Based (Hardware or Software), Cloud Based Controller without changing the Hardware.	
21	Access Point should support Dual Stack (IPv4 & IPv6), IEEE 802.1Q, Band Balancing, QoS, Layer 2/3 & 4 Access Control List.	
22	Access Point should be able to act as WIPS Sensor, Location Analytics Engine & Network Analytics Engine.	
23	Access Point should support Flexconnect or Site-Survivability, in case the controller goes down the Access Point must be able to handle the client traffic without any disruption.	
	Security & Monitoring	
24	Access Point should support AES Encrypted GRE Based Tunnel for Data Forwarding.	
25	Access Point should support auth/encryption methods for WLAN configuration: WPA-2 AES, PSK, WPA3, WPA2/WPA3 Mix, OWE. It should support Role Based Access Control, Rate-Limiting, Device Fingerprinting and 802.11r Fast Roaming.	
26	Access Point should support WMM Power Save, Tx Beamforming, LDPC, STBC, 802.11r/k/v, Hotspot 2.0, Captive Portal and WISPr.	
	Management Features	

27	Access Point should have administration access trhough HTTPS GUI, SSH & CLI. It should provide WLAN Configuration for standalone operation and provisioning tools for controller/ cloud operations. If controller dis-allows GUI/CLI access it should follow the same policy/ rule.	
28	Access Point should have recovery SSID for easy access to Console (CLI) when the AP is unreachable through network.	
	Certification	
29	Access Point shall conform to UL-2043 Plenum, EN 62311 Human Safety/ RF Exposure, WEEE & ROHS Standard.	
30	Access Point shall conform to TEC EMI EMC Standard EN/IEC 61000-4-2, EN61000-4-3, EN61000-4-5.	
31	All Switches, Optical Transceivers, Wireless Controller and Wireless Access Point should be from the same OEM for better interoperatibility, ease of administration and ease of technical support.	

WiFi 6 Outdoor WiFi Access Point

WiFi6 Outdoor WiFi Access Point		
S.No.	Specifications	Compliance (Yes/No)
1	The APs should support IEEE 802/11a/b/g/n/ac/ax standards with Dual Band Concurrent 2x2:2 streams (2.4GHz) + 2x2:2 streams (5GHz)	
2	The proposed access point should be 802.11ax (Wi-Fi 6) and Operate in dual band radio.	
3	The AP Should supports on both bands for the capacity of 2.4GHz 802.11b/g/n/ac/ax 574 Mbps and 5 GHz 802.11b/g/n/ac/ax 1200 Mbps	
4	The AP shall have 1 ports, auto MDX, auto-sensing 10/100/1000 Mbps, RJ-45 port	
5	The access point should be capable to be managed as standalone or through Hardware/virtual controller/Cloud based controller or it should work as a controller based on the site requirement.	
6	The Outdoor AP should support 40 MHz channelization on 2.4GHz and 20/40/80 MHz channelization on 5 GHz. It should also support MU-MIMO.	
7	The access point should be able to operate in full MIMO mode with 802.3af/at POE.	
8	Antenna should dynamically choose antenna patterns in real-time environment to establish the best possible connection with every device. Should support at least 64	

	antenna patterns combinations.	
9	AP should have adaptive antenna technology for performance optimization and interference mitigation features. Antenna should provide better coverage and performance utilizing multi-directional antenna patterns and polarization diversity with maximal ratio combining .	
10	Since the WLAN network will be using an unlicensed band the solution should have mechanisms that reduce the impact of interference generated by other radio equipment operating in the same band. Please Describe techniques supported.	
11	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.	
12	The antennas to be dual polarised and should be integrated inside the access point enclosure to minimize damage and create a low profile unit that does not stand out visually. The antennas could be omnidirectional or directional as per the requirement or site survey done by the vendor.	
13	The access point should support 802.1q VLAN tagging	
14	The access point should support WPA2/3 enterprise authentication. AP should support Authentication via 802.1X and Active Directory.	
15	Implement Wi-Fi alliance standards WMM, 802.11d, 802.11h and 802.11e	
16	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.	
17	Channel selection based on measuring throughput capacity in real time and switching to another channel should the capacity fall below the statistical average of all channels without using background scanning as a method.	
18	Should support Transmit power tuning in 1dB increments in order to reduce interference and RF hazards	
19	Device antenna gain (integrated) must be at least 3dBi.	
20	AP should support AES encrypted GRE-based tunnel for data forwarding.	
21	AP Should support auth/encryption methods for WLAN configuration: Open, WEP, WPA2-AES, PSK, WPA3-SAE, WPA3-OWE, IEEE 802.1X/EAP, AAA, AES-GCMP-256.It should also support Role-Based Access Control, rate-limiting, device fingerprinting, 802.11w MFP and 802.11r Fast roaming.	
22	Should support 500 or more clients per AP and SSID up to 15 per radio	
23	Should support IPv6 from day one	

24	For troubleshooting purposes, the administrator should have the ability to remotely capture 802.11 and / or 802.3 frames from an access point without disrupting client access.	
25	Operating Temperature:-20°C to 65°C	
26	Operating Humidity: up to 95% non-condensing.	
27	The Outdoor AP should be IP67 rated & Wind Survivability Up to 266km/h (165 mph)	
28	Should be WiFi certified, and WPC approved; ETA certificate and TEC certificate to be enclosed	
29	Certifications Wi-Fi Alliance: Wi-Fi CERTIFIED a, b, g, n, ac Wi-Fi CERTIFIED ax WPA, WPA2 and WPA3 WMM, Wi-Fi Vantage Passpoint	
30	Regulatory Compliance EN60950 Safety/Equivalent Indian Standard EN60601 Medical/Equivalent Indian Standard EN 62311 Human Safety/RF Exposure /Equivalent Indian Standard ROHS UL 2043 Plenum	
31	Warranty & suppory: 5 years advance replacement warranty and 5 years OEM 24/7 TAC support	

AAA for 1500 users with 4 devices each

AAA for 1500 users with 4 devices each			
S.No	Description	Features	Compliance (Yes/No)
1	Make	Please specify the make and model	
		The offered solution can be onprem or cloud based. In case of onprem solution, server to be supplied by the bidder with all the necessary Operating system, required RAM ,CPUs to cater the required number of devices mentioned in the subsequent clause.	
2	Functionality	Solution should support Authorisation, Authentication & Accounting (AAA), network access control (NAC), BYOD and Guest Access by incorporating identity, physical/device information and conditional elements on a single platform.	

		Should support variety of authentication methods (802.1 X, MAC auth and web auth) for Wired and wireless networking equipment.	
		Solution should support up to 1500 users with 4 devices each from day 1. Licenses/Subscription to be considered accordingly.The solution should be scalable to support 10K users or more in future.	
		Solution should provide facility for phased implementation approach by starting with role based access management and later incorporating end point health of security measurement.	
		Solution should support RADIUS server for client device authentication and TACACS+ for network device authentication with logging.	
		Solution should have device profiling functionality	
		Solution should have integrated support for Microsoft windows end points for health and posture assessment check to ensure only users complying to policy defined by administrator are allowed to connect on the network.	
		Authentication or authorization support for LDAP, AD, SAML 2.0 & O Auth	
		The solution should have the following features	
		Built-in guest management and device/user on boarding.	
		Web based management interface with dashboard.	
		Reporting and analysis with custom data filters.	
		Data repository for user, device, transaction information.	
		Rich polices using identity, device, and health of conditional elements.	
		Integrated network based device profiler utilizing collection via SNMP, AD, and HTTP.	
3	BYOD	Support for popular smart devices and traditional computing platforms.	
		Ability to support iOS and Android.	
		The system should correlate user, device, and authentication information for troubleshooting and tracking purposes. It	

		should offer a high-level overview of the devices on the network and their associated users.	
		The system should support automated device onboarding, allowing for secure access through a self-service portal.	
		The system should be able to integrate with Active Directory, allowing authentication of BYOD users based on their identity and device attributes.	
4	Guest Access	Solution must be capable of providing	
		Self provisioned Guest access users should be available from day one.	
		Ability to send automated SMS or email credentials to the guest users.	
		Solution should provide at least 5000 SMS for (OTP) based authentication from Day 1	
		The system should allow for the configuration of account details, including time frames and bandwidth limits. Once the account's time frame expires, the user account should automatically become inactive.	
		Solution must be capable of providing advertising services.	
		Guest solution should manage the individual guest credentials in database.	
		Ability to perform caching of MAC address post guest authentication to avoid the need for guest to re-authenticate during the period of their visit.	
		The solution should support auto-login for the self-registration workflow, eliminating the need for guests to retrieve account credentials from SMS or email for their initial login.	
		The solution should support bulk import of guest accounts and provide the capability to send credential notifications via email.	
		A post-login session statistics page should be displayed to users, allowing them to monitor their usage of the assigned quota.	
		The solution should feature a location-based captive portal that displays different landing pages depending on the guest's	

		network connection location.	
		The solution should offer fully customizable self-registration pages for guest account creation.	
5	Licenses/Subscription & support	5 years	
6	Mandatory compliance	All switches, WiFi, WLC, Transceivers, AAA should be from the same OEM for better interoperatability, management and support.	

Firewall

ATC features	
The Proposed Solution should support Web management, CLI management & should have dedicated Management Port (RJ45) from day one.	Required
Firewall should have the fesability of PoE/PoE+ ports in the appliance to power up PoE devices like Acces points, without any external dependency.	Required
Firewall should support non-repudiation to strengthen logging data security/privacy	Required
Should have built in zero trust network access funtionality in additon to VPN. Should support DNS security , OEM should offer it sown DNS servre IP's that can add as an intital layer of DNS security.	Required
Must have SD-WAN capability and have feature to create SLA profile with Jitter,Latency,Packet Loss. And same should be demonstrated by OEM/Vender in post bid POC if requested.	Required
SDWAN feature must have source,destination,service,application and users base policy creation capability. Also shuld be able to load balance or load share traffic across multiple gateways on the basis of SLA paramaters. And same should be demonstrated by OEM/Vender in post bid POC if requested.	Required
NGFW Firewall Should have Pre-defined dashboards for Traffic, Security, and User behaviour analysis report. Granular Web & Application usage reporting, Network & Threats (IPS, TP, Wireless), VPN, Email,	Required

Compliance like HIPAA, PCI, GLBA, CIPA reports and Export reports as HTML, PDF, Excel.	
The solution should support Active Directory, eDirectory, RADIUS, LDAP and TACACS+, Server authentication agents for Active Directory SSO, STAS, SATC, Single sign-on: Active directory, eDirectory, RADIUS Accounting.	Required
Azure AD integration, Support for creating users with UPN format for RADIUS authentication.	Required
Firewall should support TLS 1.3 inspection of encrypted traffic. If required bidders should showcase same	Required
If required, all technically qualified bidders should showcase the product capabilities through a demonstration at our premises	Required
OEM Should be SOC2 Type 2 compliant	Required
OEM Should be ISO 9001 & ISO 27001	Required
The OEM should not have been blacklisted by any State & Central government and PSU within the last 5 years.	Required
The NGFW Firewall OS family or Hardware should be certified under security related functions EAL4+,ICSA Lab Firewall Certification, MTCTE certification from TEC.	Required
Manufacturer Authorization (MAF), Make In India OEM Letter, Escalation Matrix for Support	Required
Make In India OEM Letter, should be class 1 MII.	Required

EPBAX / IPBAX System

1	IP-PABX System	compliance	Remarks
1	IP-PBX System should initially equipped with 16 Analog Trunks, 08 ISDN PRI Trunks, 400 Analog Extension and 40 IP extensions. System should be further expandable up to 1200 analog extensions and 2000 IP/SIP users by simply adding the required modules on the single chassis. The systems should have 100% redundancy for power supply and CPU card to ensure uninterrupted operation and also supports 15 conferences of 3-		

	participants at a time.		
2	The IP-PBX/PABX/Communication System shall employ IP at its core with IP switching technology and 100% non-blocking.		
3	The system should be IPV6 ready.		
4	Preference would be given to the indigenous design manufacturer and made in India product.		
5	The system should have VoIP and VMS at its core i.e. VoIP and VMS modules should be mounted on the CPU.		
6	The system shall provide IP functionality at its core to support SIP/IP extensions and trunks over SIP protocol. It should be possible to support SIP Trunks and SIP/IP extension with the single VoIP module. It should support license-free 99 SIP trunks and 2000 SIP/IP users (SIP/IP Phone, Mobile softphones, UC Client).		
7	It should be possible to reach the capacity of the system to 1200 analog and 2000 IP users without any add-on CPU or chassis/hardware platform.		
8	The architecture of the system shall be capable of seamless migration to its maximum capacity by simply adding peripherals cards/modules in the same chassis without compromising function/features of the system. The architecture should be non-stackable eliminating individual power supply for each chassis.		
9	The system should have an universal slot architecture and modular design to enable seamless scalability, by adding the desired necessary modules and cards as and when required. Any interface peripheral card can be inserted in any slot of the platform, whereby it is possible to increase or decrease the trunk lines or subscriber lines of the system as per the requirement.		
10	VoIP and VMS should be Daughter-board modules mounted on CPU. No slots should be utilized for it. VoIP module(s) should support up to 248 VoIP channels, 99 SIP trunks and 2000 SIP/IP users (SIP/IP Phone, Mobile softphones, UC Client). The system should have a high-density VoIP module of 64 channels to save on real-estate.		
11	System power supply should be built-in and SMPS type with input ranges from 100 – 240 VAC, 47-60 Hz OR 48VDC +/- 15%		
12	It shall have distributed processing architecture, SLIC and SMT Design.		
13	It should support up to 248 IP-TDM calls and 500 IP-IP calls (without transcoding in Relay RTP Mode) and 55 IP-IP video calls (without transcoding).		
14	The system should support UC Clients with following UC features: Presence and IM,		

	Video Calling, IM to SMS and vice versa SMS to email and vice versa, Bulk Messaging, Busy Lamp Field and SMS on No Reply, Drag and Drop conference on Windows UC Client		
15	The system should support SNMP, which helps to manage and monitor network elements, audit network usage and detect network faults. SNMP manager should support SNMPv1/v2c/v3 versions.		
16	It should support SIP over TLS and SRTP to ensure VoIP call security over IP network.		
17	System should have two Gigabit Ethernet ports for LAN and WAN to separate out local and VoIP traffic on the external network.		
18	It should be suitable for DTMF as well as the FSK type of telephone instruments.		
19	The EPABX capacity shall be suitable to scale up to 99 VoIP (SIP) Trunks and 2000 SIP/IP Users.		
20	It should have built-in multi-party conferencing without any software licensing. It should be possible to carry out 15 conferences of 3-participants at a time. The maximum number of participants required in a single conference would be 21.		
21	The system shall have the built-in Auto-attendant facility and shall be able to answer minimum 11 calls simultaneously and should support dial-by-name.		
22	The system shall be compatible with ISDN PRI line of Local Service Provider.		
23	The PRI card should be software programmable for TE/NT mode.		
24	The system shall have multiple port interfaces such as analog extension lines, digital key phone, GSM/3G/4G for voice, T1E1 PRI, RADIO, CO and E&M . All interfaces except VoIP and VMS shall be in the form of expansion cards and can be plugged into the universal slots of the system as and when required in the future. VoIP and VMS Board module should sit on the CPU.		
25	The EPABX should support Radio Connectivity in the form of a card which should be pluggable to the system.		
26	Following radio interfaces shall be interoperable: 1. MOTOROLA analog and digital radios. 2. TADIRAN RT 6001/PRC 6020 (HF) 3. TADIRAN RT - 7330M VHF 4. STARS V MKII 25 W It should have a minimum 4 radio interface port per card. It should support HF/VHF/UHF with the same radio card.		

27	The system should have an in-skin GSM card so that the multiple SIMs can be inserted on the GSM card plugged onto the PBX platform. Hence, the calls on GSM mobile can be routed through this SIMs and contribute in reduction of overall calling charges.		
28	The system should have combo cards (PSTN+ANALOG) to have flexible configuration and save on the resources of universal slots.		
29	The system should support SMPP protocol to send/receive SMS using in-skin GSM SIMs within IP-PBX. Any software required to send/receive SMS shall also to quote separately.		
30	The system shall have a USB/Ethernet port for SMDR/PMS/CAS Interface.		
31	The system shall have built-in web based software programming tool for system administration.		
32	The system shall have a built-in remote maintenance facility. The system can be programmed remotely over the internet without any modem required on the system side.		
33	The call ringing sequence would be programmable and have options such as simultaneous, hunting off, round robin and delayed simultaneous.		
34	Detailed reports of all system parameters should be generated through the SMDR port of the system.		
35	The offered system should be QSIG ready (for PRI) for Networking and Feature Transparency between two or more exchanges. System should be networked over PRI QSIG with an option of direct fiber optic connectivity on E1 PRI Card.		
36	Each port of the system shall be programmable. It shall have programmable features port-wise/extension-wise.		
37	The system shall support flexible numbering for extensions such as it may have extensions with 1 digit, 2 digits and up to 6 digits numbers as well as in combination of all.		
38	Access codes, system timers and access to features shall be programmable.		
39	Storage of outgoing, incoming and internal call reports shall be generated on the SMDR port of the system. It shall also be available online through Ethernet Port.		
40	The system should have built-in outgoing Call Log buffer of 9000 calls, incoming call log buffer of 9000 and call log buffer of 1500 internal calls.		
41	System should support dial from the corporate directory. There shall be minimum 2900 numbers possible to store in the corporate directory and shall also be possible to dial it		

	as an abbreviated number.		
42	Features given to an extension shall be accessed from any other extension by dialing the feature access codes.		
43	The system must have following features: Call Budget on Trunk, CLI based DISA (Mobile Extension), GSM Trunk Connectivity Multi-stage Dialing, Returned Call to Original Caller (RCOC), Automatic Call to Missed (Predefined) Calls on Trunks, Dual Ring Routing of calls to only permissible legal networks (Logical Partitioning), SMDR/CDR through Ethernet Port		
44	Extension features shall have an extension to extension call, extension to central office, extension to operator, automatic call back, call transfer, call forward, follow me, executive/secretary, do not disturb, barge-in, raid, Boss ring, Priority shall be supported.		
45	Operator features shall have the assistance to extension, attended call transfer, call intercept, indication of call waiting, night service control etc. should be available by default.		
46	The system shall have features as CLI based routing, call duration control, least cost routing i.e. time, number or combination of both.		
47	The system shall have a conversational recording in the mailbox. Conversation recording should be possible on Analog/Digital/IP as well as Mobile SIP Smartphones (Android/iPhone) without any additional software licenses.		
48	Varied types of open SIP Terminals such as IP Phone, SIP softphone, Mobile SIP Client and UC Client shall be supported.		
49	System's UC Client should support 1000 DSS, 500 BLF and drag & drop conference.		
50	The system should have OEM manufactured UC Client applications for Android and iPhone and on Windows PC so that the mobility can be extended for the Smartphone users as well as for Laptop/PCs users.		
51	The system should have IP Extension Bulk Configuration		
52	The system must support the following features of IP telephony: Dynamic DNS, Registrar Server, Proxy Server, Presence Server, NAT and STUN.		
53	The system should support Voice Mail System with following features: Attend as much as 64 calls simultaneously with flexibility of routing callers to desired extension or delivering information depend upon the selection, Dial-by-Name to reach the intended user directly without knowing/remembering extension number, Selectively allocate		

	voicemails to users with the flexibility of customizable mailbox size and greetings for All/Selective users, Group mailbox to share messages between departmental groups, Anywhere access to voicemail with just a phone call, Password protected secured voice mail access, Record important conversations for future reference and record maintenance, Redirection of voice mails to another extension in case of non-availability, Tag voicemails while Forwarding Messages to Another Mailbox, Broadcast voice message to a group of personnel simultaneously, Distribution lists for delivery of voice mails to different set of users or groups, Message wait indication via ring, change in dial-tone, voice message or message wait lamp, Notification of a new voicemail via email alert or a phone call, Mailboxes for all users (Analog / Digital / IP / UC users)		
54	All the peripheral cards (extension cards, trunk cards) should be hot-swappable. i.e. it should be possible to replace a peripheral card while system power is on.		
55	The systems should be redundant which offer 100% duplication of power supply and CPU card. In the event of failure of the main power supply or CPU card, the standby will take over without disruption of on-going calls.		
56	Vendor must have a ZED Certified MSME organization.This Certification has been issued to organization by Quality Council of India.		
58	OEM should have existing capability and infrastructure to provide technical support as well as their own factory in India.		
59	OEM should be a registered business entity in India with their own office in India. Submit Certificate of Incorporation under the provisions of companies Act, 1956.		
60	As per DOT PPO No. 18-10/2017-IP, dated 29th August 2018, OEM has to submit following documents: 1) The Intellectual Property Right (IPR) resides in India for Hardware Design, (b) The Copyright is in India for the software Design & Development.		
61	The products must be researched, designed, and manufactured in India. The OEM must have its own in-house, government-registered R&D facility in India, and should not outsource any development or research activities, submit the undertaking on OEM Letterhead. Also, R&D registration certificate issued by a government body must be attached as proof.		
62	PABX OEMs must be registered on the Trusted Telecom Portal to qualify as "Trusted Sources."		
63	OEM should be PLI-certified Indian brand that focuses on quality and innovation.		
64	The products should qualify under CLASS- I LOCAL SUPPLIER as per Preferential Market Access (PMA) and Public Procurement Policy (PPP) Make in India (MII) scheme of the Govt. of India dated. 04.06.2020 & 16.09.2020 with 50% or latest applicable local content as per the Govt. norms.		

65	OEM should have ISO14001, ISO 20000, ISO 27001, ISO 45001, ISO 9001 and ROHS certificates.		
66	OEM should not be blacklisted by any Central/State Govt. Organization, PSU, Public Listed Company or Indian Army.		
67	With reference to Order (Public Procurement No. 1) issued vide No. F.No.6/18/2019-PPD dated 23rd July, 2020, OEM and Bidder should not be from such a country that shares Land Border with us. OEM and Bidder should submit the declaration against this clause.		
68	Proposed OEM should have dedicated, toll-free telephone numbers for after-sales support.		
69	As per Mandatory Testing and Certification of Telecommunication Equipment (MTCTE) guidelines, PABX System and all Phones should be TEC ER Certified. OEM to submit the certificates.		
2	Specification for Type-2 IP Phone	compliance	Remarks
	· 2 x 10/100/1000 Mbps LAN & PC Ports · Graphical LCD with Backlit · LED for Incoming/Ongoing Call, Mute, Hold · Add on 32 key module support, maximum key modules shall be supported · Intuitive User Interface with Icons · Multiple Languages Caller ID with Name, Number · 45 or more keys including 4 Context Sensitive Hard Keys · RJ9 Handset Port,RJ9 Headset Port,3.5 mm Headset Port · Installation: Wall Mount, Table-top · CE,FCC-15,RoHS, Power over Ethernet (IEEE 802.3af) · Power Consumption: 5W (Typical) · Connector: DC Power Jack, 5VDC/600mA · Operating Temperature Range =0 to 45°C · Storage Temperature = 0 to 55°C · Message wait Lamp, Ringer Lamp, Voice Mail, Call Pickup– Group and Selective, Paging		
	Phone Features: · Mute, Call Hold, Do Not Disturb, Speed Dial, Hotline, Redial, Call Back, Auto Answer, Call Forward, Call Waiting, Call Transfer, Room Monitoring, Conference, Directory, Call Logs, Paging Dial-by-Name		
	Certification: CE, FCC, EMI- EMC, SAFETY, ROHS, TEC-ER		

End of Document