Kerala Institute of Tourism and Travel Studies (KITTS)
Residency, Thycaud, Trivandrum – 14
Ph: 0471 – 2329539, 2329468

Invitation for Tender for the setting up of Wi-Fi Connectivity in KITTS campus

No.1608/KITTS/Wi-Fi/2013 06.12.2013

Sealed tenders are invited from reputed agencies for setting up of Wi-Fi connectivity in KITTS campus at Thycaud, Thiruvananthapuram. Interested parties are directed to submit their tenders (technical and financial bid) to the Office of KITTS, Thycaud, Trivandrum as per the following technical specifications attached to the tender.

Quality certificate to be attached with the Technical bid. Technical bid should be accompanied along with Rs.5000/- EMD by DD in favour of Director, KITTS payable at Trivandrum.

Conditions

Rates should be firm for a period of 1 year
Installation – KITTS, Main Office, Trivandrum

Those who are unable to supply and install the same within the stipulated time after issue of work order will be black listed. The cover of the tender should be marked "Tender for setting up Wi-Fi connectivity at KITTS". The tender must consist of technical and financial bid and should be submitted in separate covers. Those tenders which are not submitted in two covers will be rejected. The financial bid will be opened for those tenders who satisfy the terms and conditions of the technical bid. The financial bid should contain amount for surety of items and setting up Wi-Fi connectivity. The final amount will be taken for comparison of financial bid.

Last date for submitting sealed tenders: 27.12.2013 on or before 2.30 pm and opening of tender at 3.00 pm on the same day.

Director

Components and specifications required for setting up Wi-Fi connectivity in KITTS campus

Active Components

Sl.No.	Component specification	quantity
1	Redundant Wireless LAN Controller Cluster with license for up to 48 Access Points	2
2	a) Type 1 Access Point with inbuilt antennas b) Wall Mount Bracket for Type 1 AP's	34
3	a) Type 2 Access Point with 3 x external antenna connectors b) Dual-band 802.11n outdoor omni-directional antenna for Type 2 AP c) Lightning arrestor for outdoor antenna installation	4
4	Firewall with 16 x 10/100/1000Base-T Ports + 4 slots	2
5	a) 12 Port PoE+ 10/100/1000BaseT + 2 SFP uplink switch b) 24 Port PoE+ 10/100/1000BaseT + 2 SFP uplink switch	3
6	NMS to manage and support all of the above devices	1

Sl.No.	Component specification	quantity
1	Single Mode Fiber Transceiver SC type	4 No's
2	12u wall mount rack. Power supply, Fan and hardware packets.	1 No.
3	6U wall mount rack. Power supply, Fan and hardware packets.	2 No.'s
4	Optical Fiber Cable 6 core Outdoor - Armoured Jelly filled Loose tube Single Mode	400 meters
5	12 port LIU (with splice holder, SC adapters/couplers)	3 No's
6	SC Pigtails Single - 1 Mtr	36 No's
7	Single Mode SC Duplex Patch cord	6 No.'s
8	CAT6 UTP Cable 23AWG Solid	8 boxes
9	Cat 6 Information Outlet with SMB	38 No's
10	24 Port Cat6 Rack Mount Patch Panel.	3 No's
11	Cat 6 patch cord - 1 Mtr	38 No's
12	Cat 6 patch cord - 2 Mtr	38 No's
13	25mm PVC Conduit/Casing and capping	1000 meters
14	HDPE Pipe	350 meters
15	OFC Cable Marker	5 No's

Passive Components

Specifications of components related to setting of wi-fi campus

- **Wireless Controller with Indoor and Outdoor Access Point**

Hardware Description/ Compliance
Redundant Wireless LAN Controller Cluster with license for up to 48 AP's
WLAN Controller should have minimum 4 x 10/100/1000BaseT ports and 4 x SFP ports
WLAN Controller should have inbuilt redundant power supplies
Two types of AP's are required for the network.
Type 1 AP
WLAN Access Point should be an indoor Dual Radio AP with 802.11a/n (5GHz) and 802.11b/g/n

(2.4GHz) concurrent operation
WLAN Access Point should have Internal omni-directional antennas
AP should support MIMO with 2 radio transmit and 2 radio receive chains
AP should support minimum 2 spatial streams
AP should be Safe tamper-proof design with completely sealed enclosure and no visibile external antennas
AP should not have any data, security credentials, or encryption keys stored locally
AP should not have a console port to ensure local access is not possible
AP should have one 10/100/1000BaseT PoE port
AP should have provision to securely mount the access point with anti-tamper screws to avoid theft
AP should support both roof mount and wall mount installations since some of the rooms in the institute have very tall roofs and it might be required to do a wall mounting in these cases
Wall Mount kit should have provision to extend the AP from the wall so as to safely install without having a very sharp Ethernet Cable bend radius
Type 2 AP
WLAN Access Point should be an indoor Dual Radio AP with 802.11a/n (5GHz) and 802.11b/g/n (2.4GHz) concurrent operation
Access Point should be a UL-2043 plenum rated model with external antenna ports for use with indoor or outdoor antennas
AP should support MIMO with 3 radio transmit and 3 radio receive chains
AP should support minimum 3 spatial streams
AP should not have any data, security credentials, or encryption keys stored locally
AP should not have a console port to ensure local access is not possible
AP should have one 10/100/1000BaseT PoE port
AP should have provision to securely mount the access point with anti-tamper screws to avoid theft
AP should support both roof mount and wall mount installations since some of the rooms in the institute have very tall roofs and it might be required to do a wall mounting in these cases
Wall Mount kit should have provision to extend the AP from the wall so as to safely install without having a very sharp Ethernet Cable bend radius

Feature Description
WLAN Solution should supports the use of the 802.1X protocol for user authentication for Identity based networking (AAA)
The system should support RADIUS as a backend identity store for wireless user authentication, mac authentication and admin authentication.
Should support multiple servers and support requests to be load balanced between available servers.
Should support RADIUS accounting for reporting on wireless session activity (including roaming events), system logging, admin authentications, SIP call detail records and cli command auditing.
Should support supports RADIUS proxy for complex RADIUS deployments
Should support use of LDAP identity stores for user authentication
To enable identity based networking without the use of an external identity store, the system should support local configuration of users

and mac addresses for authentication.
When supporting mac authentication for wireless sessions the system should supports the definition of a mac address range to define a set of mac addresses
To enable additional control over authentication and authorization the WLAN solution should supports policy to override attributes returned from AAA based on: AP, port, SSID, time-of-day, vlan or user.
Should support RADIUS Ping to allows the operator to send a simulated RADIUS authentication or accounting message to a RADIUS server to verify server configuration.
The system should support limiting the number of active sessions allowed for a single identity.
Physical ports on the WLAN Controller should support wired 802.1X authentication using the same policy and attributes supported for wireless sessions.
The Wireless LAN Controller should support "chaining" multiple authentication methods requiring a session to pass all authentication methods before being granted access to the wireless network.
The Wireless LAN Controller should have a captive portal system to authenticate wireless and wired users via a web browser.
The Inbuilt Web Portal Authentication should support a completely customizable captive portal experience including user login and 'click-thru' authentication. Configurable to be delivered either via https or http.
Wireless LAN Controller should support redirecting to external captive portal authentication systems where the external server uses RADIUS CoA to authorize the session on the WLC.
Based on awareness of the local rf environment, access points in the WLAN solution should be capable of automatically optimizing radio tx power configuration.
The WLAN system should have ability to detect and compensate for coverage holes introduced by AP failures.
Based on awareness of the local rf environment, access points in the WLAN solution should be capable of automatically optimizing radio channel configuration
After auto tuning the channel for a specific period of time, the system should allow the optimized channel and power plan to be converted to

static system config.
The system should allow for individual control over the supported and advertised 802.11 data rates for an individual SSID.
The access point should support up to 32 SSIDs per radio. Individual SSIDs should be capable of supporting multiple authentication methods and provide complete isolation between SSIDs on the same radio.
Should support configuration of an AP in the WLAN solution to be put into a mode of dedicated spectral graphing to allow visualization of spectrum using a management tool.
All AP's providing client services should be capable of simultaneously scanning for and identifying common sources of rf interference.
The WLAN solution should support wireless backhaul of the AP control channel allowing for mesh topologies up to 4 nodes deep.
The WLAN solution should support bridging two wired networks via an AP-AP bridge with up to 4 wireless hops.
The access point should suports receiving 11n A-MSDU aggregates from 11n clients.
The WLAN Solution should support the use of 802.11n standard Transmit Beamforming to optimize the Access Point to Client data path.
WLAN Access Point should be capable of remote site operation where Access Point to Controller latency is up to 2 seconds.
WLAN remote AP should support configuration of a backup SSIDs which should become operational during WAN outage
Access points in the WLAN solution should be capable of forwarding traffic directly at other AP's bypassing the controller.
Controllers in the WLAN solution should be capable of establishing VLAN tunnels to other Controllers to provide remote VLAN access to wireless clients.
WLAN AP's should be capable of initiating VLANs tunnels directly to other APs (or controllers)
The WLAN Controller should support PMK caching enabled fast roaming as outlined in 802.11i

To enable coordination of users, APs, security and VLANs across a WLAN installation, the WLAN system should support grouping controllers into a single management domain to facilitate the sharing of information.
The WLAN solution should provides layer-2 transport for users on the system, which allows for transport and fast roaming of IPv6 enabled clients/traffic.
When Access Point forward data bypassing the controller, the ACL support should be distributed to the AP for consistent enforcement
For mulitcast traffic optimization, the WL solution should support IGMP Snooping. The system should learn stream registrations and only distribute multicast packets to APs with active subscribers.
The WLAN solution should Spanning Tree Protocol and for faster convergence, Spanning Tree support should also includes the Backbone fast and Uplink Fast options for individual ports.
The WLAN system should support the ability to identify L3 multicast traffic and convert it to L2 unicast frames for reliable delivery over the air.
The WLAN ACL system should support the ability to filter IPv6 traffic
The WLAN filter system should identify and filter inbound IPv6 Route Advertisements from user sessions.
The WLAN solution should support clustering of controllers to create a highly scalable solution.
The WLAN Virtual Chassis cluster configuration should provide a single point of config for all of the controllers in the cluster.
Proposed solution should be capable of supporting up to 512 access points either by adding additional controllers to the cluster or adding licenses on the current controller
APs in the WLAN solution should support the detection of non-system access points in the vicinity of the WLAN system and the detection of rogue devices should happen concurrently with user service.
WLAN Controllers and APs should have ability to monitor the wire for AP and client mac addresses and provide correlation between wireless and wired traffic to allow for additional classification options.
Should support Rogue suppresion by ensuring that devices which have been classified as "rogue" are subject to over-the-air device containment.

When scanning for devices the system should have ability to passively scan channels outside of the configured regulatory domain.
The Access Point and Controller should have ability to monitor activity for a set of common wireless based DoS and intrusion events and have option to blacklist offending stations and prevent further communication with the WLAN system.
When operating in the vicinity of other WLAN systems the WLAN solution should have option to configure a whitelist of neighboring systems.
For known rogue devices, the system should support configuration of a rogue blacklist that ensure that devices are immediately classified as rogue devices in the system.
The Controller to management station communication should be via a named user account or authenticated against RADIUS.
The WLAN solution should support the Robust Security Network as defined in the 802.11i specification and should be WPA2 certified by the WiFi Alliance.
The WLAN solution should support the WiFi Protected Access as defined in the 802.11i specification and should be WPA certified by the WiFi Alliance.
The system should support the use of WEP encryption and also support Dynamic WEP for use with 802.1X users.
The system should supports the use of CCMP and TKIP encryption.
The system should support the use of Pre-Shared Key authentication.
The system should allows configuration of SSIDs to enforce the use DHCP for all connected wireless clients.
To prohibit peer-to-peer traffic on wireless networks the system should support blocking of all communication between associated wireless clients.
The Controller should support the inspection of device traffic to allow the system to identify the type of device accessing the network e.g. iOS, Android, Windows and allow policy attributes to be applied based on the type of device.
Should support feature to assign a user session on the WLAN system to an individual qos-profile which can limit per session bandwidth usage.
Should support configuration of an SSID with a strict bandwidth limit.

The WLAN solution should support standard Proxy ARP.
The WLAN solution should support UAPSD power save functionality as defined in the 802.11e specification.
The controller should support a configurable limit of sessions allowed on an SSID (on a pre-radio basis)
When a WLA detects clients on both the 2.4 and 5 Ghz bands, the system should have abilty to steer to the 5Ghz band.
The Access Point should have ability to monitor the system for active voice or video streams and reduce the frequency of WIDS/WIPS scans to minimize impact to call quality.
When the Access Point receives packets marked with DSCP information, the system should preserve this marking on the tunneled packets to the controller and should support this for IPv4 and IPv6 traffic.
When configured for local forwarding by bypassing the controller, the access point should have ability to mark 802.1p bits according to priority before transmitting on the wire.
The system support manual configuration of CoS to DSCP marking for mapping CoS at the AP. Supports IPv4 and IPv6 traffic.
The AP should support feature to disable the visible LEDs on the platform to have "lights out" mode of operation
The AP support a beacon mode where the visible AP leds will blink in a fixed pattern for easy identification of an AP.
The WLAN system should supports a simple web based interface for simple device configuration.
The controller should support a method of device configuration where the controller will discover a WLAN NMS installation and have configuration automatically pushed to it.
The WLAN system should support telnet and SSH for access to the CLI.
The system should supports the configuration of the number of AP's which are simultaneously upgraded during a software upgrade.
The WLAN system should support LLDP for device discovery and management.
The system should support a simple CLI and Web based system quickstart configuration for initial device configuration.

The system should support a configurable Message-of-the-Day and Banner and the notification should support configuration to require acknowledgment.
The WLAN solution should provide management visibility into the IPv6 addressing used by session on the network.

- **Firewall**

Specification for Firewall/ firewall Compliance
Hardware Requirements
Modular Firewall with minimum 4 slots for expansion
firewall should have minimum 16 x 10/100/1000BaseT Copper ports
The firewall should be provided with minimum 2GB DRAM and 2GB Flash
firewalls should support modular LAN and WAN connectivity options including 1G Fiber / Copper, T1/E1 & Serial V.35
firewall should support 3G connectivity for backup using GSM and CDMA technologies
All Ethernet ports on the firewall should support L2 and L3 features
The firewall should have a minimum performance of 200Kpps with routing and firewall enabled
The firewall should support a througput of minimum 1.5Gbps and 3DES VPN throughput of minimum 300Mbps and should support minimum 1000 VPN tunnels
Hardware should comprise of all Licenses required for network commissioning.
Quality of Service (QoS) requirements
firewalls should support Class-based queuing with prioritization
It should be possible to configure maximum bandwidth and guaranteed bandwidth
firewalls should support Queuing based on VLAN, DLCI, interface, bundles, or filters
firewalls should support Marking, policing, and shaping
firewalls should support congestion management features like WRED
Routing protocol support

The firewall should support IPv4 and IPv6 routing
The firewall should support VRRP
firewalls should support IPv4 Routing features - RIP v1/v2, OSPF, BGP, BGP Route Reflector, IS-IS
firewalls should support IPv6 Routing features - RIPng, OSPFv3, IPv6 MLD, IS-IS and BGP
Should support MPLS features - L2 VPN, L3 VPN, LDP, RSVP and Circuit Cross Connect
The firewall should support Policy Based Routing, Source Based Routing and Reverse Path Forwading
The firewall should support Routing Protocols over IPSec Tunnels
Firewall should support virtualization with support for minimum 40 virtual routers
L2 Feature Support
Should support 802.1q VLAN with support for minimum 512 VLAN's
Link Aggregation 802.3ad / LACP
Jumbo Frame (9216 Byte)
Spanning Tree Protocol (STP) 802.1D, RSTP 802.1w, MSTP 802.1s
802.1x Port based and multiple supplicant authentication
Should have an internal DHCP server
Multicast Features
IPv4 Multicast features
IGMP v1/v2/v3
PIM-SM, PIM-DM
PIM- Source Specific Multicast (SSM)
Multicast inside IPSec Tunnel
Firewall & Security Features
Should support AAA using RADIUS or TACACS
Should support Packet Filters
Should have Stateful Firewalling with support for minimum 32 zones
Should support Network attack detection and support DDoS attack prevention

Should support Tunnels (GRE, IP-in-IP, IPSec)
Should support MD5 and SHA-1 authentication
Should support session synchronization for firewall and VPN
Should support TCP reassembly for fragmented packet protection and Brute force attack mitigation
Should support SYN cookie protection
Should support Zone-based IP spoofing
Should support Network address translation (NAT) with support for Source NAT with PAT and Destination NAT with PAT
Should support next generation firewalling with support for following features
Should have support for context, protocol information, and signatures used to identify atleast 900 different applications on any TCP or UDP port
Should have ability to identify Nested applications running on top of, or embedded into approved/trusted services and protocols.
Should have ability to create fine grained application control policies to allow or deny traffic based on dynamic application name or group names rather than static IP/port information.
Should have ability to identify attacking botnet traffic against legitimate client traffic based on application-layer metrics and privide remedy against these botnet attack
Should have ability to collects byte, packet, session, and time statistics on a per application level
Should be tightly integrated with an IPS solution so that the IPS can subscribe to the results of the application identification / contextualization to determine the appropriate protocol decoding and attack objects to use for the incoming traffic
Management and Troubleshooting
firewall should have Console, Telnet and Web for management
firewalls should support Software upgrades through Web
firewalls should support SNMPv2 and SNMPv3
Extensive debugs on all protocols
firewall should have flow monitoring and accounting services
firewall should have SLA monitoring features with support for Sessions, packets & bandwidth usage

- **24 Port POE Switch**

Specification for Access Switch - 24 Port/Compliance
Hardware and interface requirements
The switch should have minimum 24 x 10/100/1000 PoE+ ports and 4 x 1G SFP uplink ports
Switch should support redundant power supplies via an external RPS
Performance requirements
Packet switching capacity should be should be minimum 56Gbps for line rate performance for a fully populated switch
Switch should have minimum 41Mpps Forwarding rate
Switch should support stacking of up to 4 switches using 1Gbps Copper or Fiber uplinks
Layer 2 Switching
Switch should support minimum 16000 MAC addresses per system
Switch should support Jumbo frames – 9,000 bytes
Switch Should support minimum 1000 VLANs and VLAN ID's
Switch Should support Port-based, MAC-based, Voice and Private VLAN
Switch should support IEEE 802.1ak: Multiple VLAN Registration Protocol (MVRP)
Switch should support Multcast VLAN Registration (MVR)
Switch Should support 802.1Q VLAN tagging
Switch Should support Voice VLAN
Switch Should support Voice VLAN LLDP
Switch Should support Voice VLAN LLDP-MED with VoIP integration
Switch should support G.8032 Ethernet Ring Protection (ERP)
Layer 3 Routing
Switch should support IPv4 and IPv6 static routing

Switch should support RIPv1/v2, OSPF v1/v2 and Bidirectional Forwarding Detection (BFD)
Quality of Service (QoS) requirements
Switch should support Class-based queuing with prioritization
Switch should support Queuing based on VLAN, interface, bundles, or filters
Switch should support Marking, policing, and shaping
Switch should support WRED
Switch should support 8 hardware queues per port
Switch should support Strict priority (SP), Shaped Deficit Weighted round-robin (SDWRR) scheduling methods
System Management and Administration
Switch should support Software upgrades
Switch should support SNMPv2 and SNMPv3
Security features
Switch Should support Port-based, VLAN-based and Router-based ACL's
ACL entries (ACE) in hardware per system should be minimum 1,500
Switch should support ACL counters for denied and permitted packets
Switch should support MAC limiting
Switch should support Dynamic ARP Inspection (DAI)
Switch should support DHCP snooping
Switch should support L2-L4 ACL
Switch should support Control plane DoS protection
Services and Manageability
Switch should be managable through CLI, Web Interfce, SSHv2 and HTTP/HTTPs
Switch should support Out-of-Band management Ethernet port
Switch should support DHCP server, DHCP client, DHCP proxy, DHCP relay and DHCP helper functions
Switch should support local and remote port mirroring
Configuration backup via FTP/secure copy

- **L2 12Port POE Switch**

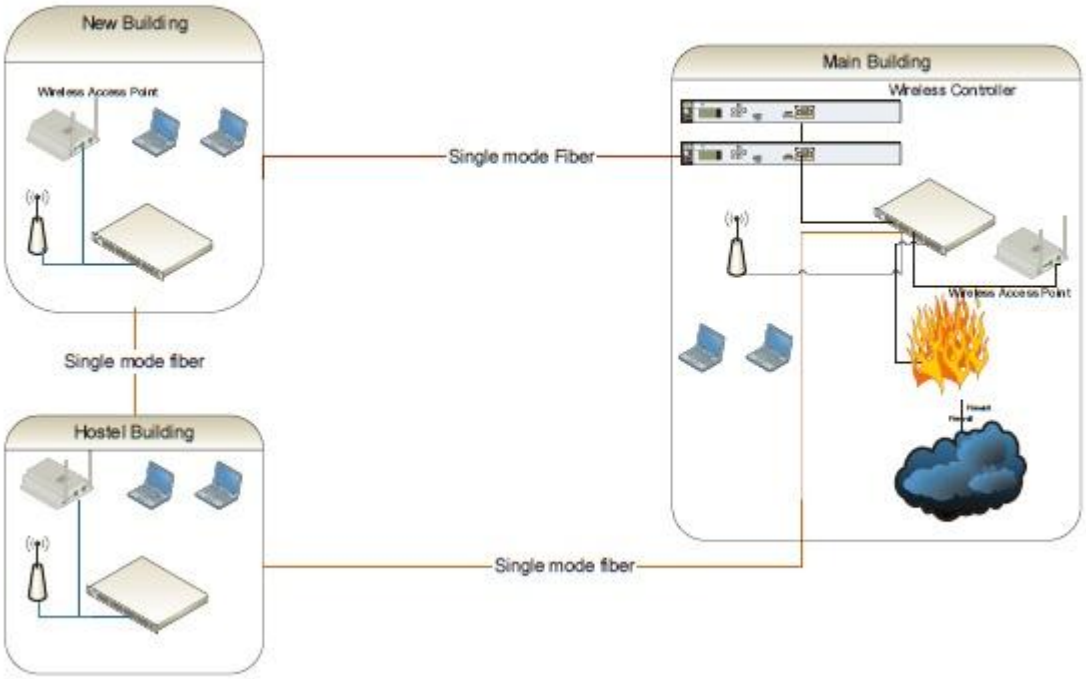
Specification for Access Switch - 24 Port/Compliance
Hardware and interface requirements
The switch should have minimum 12 x 10/100/1000 PoE+ ports and 2 x 1G SFP uplink ports
Performance requirements
Packet switching capacity should be should be minimum 28Gbps for line rate performance for a fully populated switch
Switch should have minimum 21Mpps Forwarding rate
Switch should support stacking of up to 4 switches using 1Gbps Copper or Fiber uplinks
Layer 2 Switching
Switch should support minimum 16000 MAC addresses per system
Switch should support Jumbo frames – 9,000 bytes
Switch Should support minimum 1000 VLANs and VLAN ID's
Switch Should support Port-based, MAC-based, Voice and Private VLAN
Switch should support IEEE 802.1ak: Multiple VLAN Registration Protocol (MVRP)
Switch should support Multcast VLAN Registration (MVR)
Switch Should support 802.1Q VLAN tagging
Switch Should support Voice VLAN
Switch Should support Voice VLAN LLDP
Switch Should support Voice VLAN LLDP-MED with VoIP integration
Switch should support G.8032 Ethernet Ring Protection (ERP)
Layer 3 Routing
Switch should support IPv4 and IPv6 static routing

Switch should support RIPv1/v2, OSPF v1/v2 and Bidirectional Forwarding Detection (BFD)
Quality of Service (QoS) requirements
Switch should support Class-based queuing with prioritization
Switch should support Queuing based on VLAN, interface, bundles, or filters
Switch should support Marking, policing, and shaping
Switch should support WRED
Switch should support 8 hardware queues per port
Switch should support Strict priority (SP), Shaped Deficit Weighted round-robin (SDWRR) scheduling methods
System Management and Administration
Switch should support Software upgrades
Switch should support SNMPv2 and SNMPv3
Security features
Switch Should support Port-based, VLAN-based and Router-based ACL's
ACL entries (ACE) in hardware per system should be minimum 1,500
Switch should support ACL counters for denied and permitted packets
Switch should support MAC limiting
Switch should support Dynamic ARP Inspection (DAI)
Switch should support DHCP snooping
Switch should support L2-L4 ACL
Switch should support Control plane DoS protection
Services and Manageability
Switch should be managable through CLI, Web Interfce, SSHv2 and HTTP/HTTPs
Switch should support Out-of-Band management Ethernet port
Switch should support DHCP server, DHCP client, DHCP proxy, DHCP relay and DHCP helper functions
Switch should support local and remote port mirroring
Configuration backup via FTP/secure copy

Sl.no.	Description of work	quantity	Unit
1	UTP Cable laying	2400	Meter
2	OFC Cable Laying	400	Meter
3	HDPE Pipe Laying	400	Meter
4	Soil digging and Refilling (1meter with sand and brick)	300	Meter
5	Route marker Fixing	5	Nos
6	Splicing - SC SM Pigtail	24	Nos
7	PVC Conduit laying	1000	Meter
8	I/O Termination	38	Nos
9	Patch Panel Termination	3	Nos
10	12U Rack Fixing	1	Nos
11	6U Rack Fixing	2	Nos
12	Testing and Certification	56	Lot

Details of labour involved in setting up wi-fi campus

Indoor and Outdoor Wi-Fi Solution diagram for KITTS Campus



Terms and Conditions

1. Passive and labor quantity mentioned are indicative, final quantities will be arrived after work is completed at actual
2. All active components should be from the same OEM
3. All products should be quoted with 3 year onsite warranty
4. Price quoted should be inclusive of all taxes
5. Active components should be from international reputed makes preferable such as Cisco, Juniper, HP, Aruba and for Passives components AMP, Molex, Schneider, Panduit.