Date: 23.06.2016

RailTel Corporation of India Ltd
(A Government of India Enterprise)

Plot No 143, Sector 44,
Institutional Area,
Opposite to Gold Souk,
Gurgaon, Haryana- 122003
Work: 0124-4236083
Fax: 0124-4236084

Website: **www.railtelindia.com**

Corrigendum -II

Sub: Clarification of queries for tender "**Empanelment of OEM's/Vendors for entering into Rate Contract for Access Points of various Configuration for Wi-Fi Project**."

Ref: i) This office Tender No. RailTel/Tender/OT/CO/DNM/2016-17/Wi-Fi/RC for Access Point/335 dated 13.05.2016.

1. **Clarifications for Point No. 8 of Clause 3.3.2 of Chapter-3 (Bid Data Sheet, Chapter-2 Point No. 8 of Eligibility Criteria):**

   The bidder should have annual turnover of minimum of the value Rs 12 Crores or above during the last 3 financial years excluding the current year. The bidder should provide Audited Balance Sheets and annual reports as documentary evidence or other such documents so as to establish the financial soundness of their company for the preceding three financial years.

2. **Point No. 11 of Information to bidder of Chapter-1 may be read as:**

   OEM should be figured in Gartner/IDC Report of the last three years i.e. 2013, 2014 & 2015 report for wireless LAN

3. **Clarifications for Point No. 3 and 4 of Clause 3.3.1 of Chapter-3 (Bid Data Sheet, Chapter-2 Point No. 7 of Eligibility Criteria):**

   An undertaking from OEM is acceptable in support of these points.

4. **Point No. 9 of Information to bidder of Chapter-1 may be read as:**

   OEM should have a registered office in India to provide 24x7 Technical supports for entire Access Wi-Fi Tender requirement and supplied hardware. The certificate to this effect should be submitted by bidder.

5. **Clause No. 3.11 of Chapter-3 (SPLITTING OF Quantity) has been deleted.**

6. **Point No. 14 of Information to bidder of Chapter-1 may be read as:**

   RailTel plans to procure about 25% of access point quantities immediately and balance in lots of approximately 10% quantity each in due course of the contract depending upon the business requirement of RailTel.

7. **Point No. 10 of Information to bidder of Chapter-1 may be read as:**

   Equipment offered shall have complete data sheets and detailed description on OEM web sites. The products in pipelines in final stage of rollout are acceptable.OEM should provided complete datasheet and specifications for New upcoming products on their letterhead.

8. **New Point No. 5 & 6 has been added in Clause No. 3.3.1 of Chapter-3 (Eligibility Criteria for OEM):**

   5. OEM should have installed minimum 2000 AP's in public hotspot and single order of 1000 AP's in government organization.

   6. OEM should not be black listed anywhere in the world

9. **The Modified Technical Specifications of Clause 1.1 of all Category and Cloud/Appliance based Wireless Controller of Chapter-4 may be read as:**

Technical Specifications

1. Category 1 Access Point:

Reference	Parameters	Technical specification
CT1HW1	Hardware	Access Points proposed must include radios for both 2.4 GHz and 5 GHz.
CT1HW2	Hardware	Must have a robust design for durability, without visible vents
CT1HW3	Hardware	Must include dual band antennas to support both the 2.4GHz and 5GHz operations simultaneously.
CT1HW4	Hardware	Proposed access point shall support MDO(Mobile Data offload)
CT1HW5	Hardware	Mounting kit should be standard which shall be used for mounting access point
CT1HW6	Hardware	Must Support operating Temperature of 0C to 40 C
CT1HW7	Hardware	Must support operating humidity of 10 to 90% (Non Condensing)
CT1WS1	wireless Standard	Must support 2X2 multiple-input multiple-output (MIMO) with TWO spatial streams

CT1WS2	wireless Standard	Must support simultaneous 802.11n on both the 2.4 GHz and 5 GHz radios and 802.11ac on 5ghz .
CT1WS3	wireless Standard	Must support data rates unto 800 Mbps on 5Ghz radio and 280 mbps on 2.4Ghz radio.
CT1WS4	wireless Standard	Must support 40 MHz and 80 MHz wide channels in 5 GHz.
CT1WS5	wireless Standard	Must support unto 21 dbm of transmit power or better in both 2.4Ghz and 5Ghz radios.
CT1RF1	RF	The Wireless AP should support technology to improve downlink performance
CT1RF2	RF	The AP shall be able to load-balance between 2.4Ghz and 5Ghz band.
CT1RF3	RF	Must have -90dB to -100B or better Receiver Sensitivity.
CT1RF4	RF	Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization
CT1RF5	RF	Should support configurable carrier sense threshold
CT1M1	Mesh	The Wireless Backhaul shall operate in 5Ghz
CT1M2	Mesh	Support Encrypted and authenticated connectivity between all backhaul components
CT1M3	Mesh	Access point shall have wired uplink interfaces i.e. 2X10/100/1000BASE-T Ethernet
CT1R1	Roaming	Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.
CT1S1	Security	Must support Management Frame Protection.
CT1S2	Security	Should support locally-significant certificates on the APs using a Public Key Infrastructure (PKI) or preinstalled certificates on AP for authentication
CT1S3	Security	Provision of Wireless IPS to filter malicious traffic
CT1E1	Encryption	Access Points must support a distributed encryption/decryption model.
CT1E2	Encryption	Access Points must support hardware or software based encryption
CT1M1	Monitoring	Must support the ability to serve clients and monitor the RF environment concurrently.
CT1F1	Flexibility:	AP model proposed must be able to be both a client-serving AP and Parallely monitor- Intrusion Prevention services.
CT1F2	Flexibility:	Should support mesh capabilities for temporary connectivity in areas with no Ethernet cabling.
CT1F3	Flexibility:	should support QoS for voice over wireless.
CT1F4	Flexibility:	Must support Controller-based and standalone(autonomous) deployments

CT1F5	Flexibility:	Must support 16 WLANs per AP for SSID deployment flexibility.
CT1O1	Operational:	Must support telnet or SSH or console login to Aps directly for troubleshooting flexibility.
CT1O2	Operational:	Must support automatic detection of dropped connection to controller,
CT1O3	Operational:	Must support automatic failover to secondary controller, upon detecting lost connection to controller
CT1O4	Operational:	Must support DHCP Option 82, defined in RFC 3046, including support for Sub-option 01 (Circuit-Id) and Sub-option 02 (Remote Id) fields.
CT1O5	Operational:	With Controller- (from a data-plane plane perspective) must support: - Ethernet over GRE IPv6 tunnel - Automatic detection of failed tunnel termination, with configurable connection retry and timeout. - Automatic failover to secondary tunnel termination address.
CT1O6	Operational:	Support for basic AP monitoring statistics for each radio: Bytes Sent, Bytes Received, Packets Sent, Packets Received, Radio Channel Utilization, Noise.
CT1O7	Operational:	Must support data-plane split tunneling in which ACLs may be configured to enable a range of destination netblocks and/or IPs to bypass the data-plane tunnel and be bridged on the wired interface.
CT1P1	Power:	Must support Power over Ethernet and AC.
CT1Q1	Quality of Service:	shall have the support of 802.11e and WMM
CT1Q2	Quality of Service:	Should be WiFi Alliance Certified and WPC approved and ETA certificate
CT1Q3	Quality of Service:	Must support Reliable Multicast Video to maintain video quality
CT1Q4	Quality of Service:	Must support QoS to prioritize video ,voice and Data traffic

2. Category 2 Access Point:

Reference	Parameters	Technical specification
CT2HW1	Hardware	Access Points proposed must include radios for both 2.4 GHz and 5 GHz.
CT2HW2	Hardware	Must have a robust design for durability, without visible vents
CT2HW3	Hardware	Must include dual band antennas to support both the 2.4GHz and 5GHz operations simultaneously.
CT2HW4	Hardware	Proposed access point shall support MDO(Mobile Data offload)
CT2HW5	Hardware	Mounting kit should be standard which shall be used for mounting access point
CT2HW5	Hardware	Must support operating humidity of 10 to 90% (noncondensing)
T		
CT2WS1	wireless Standard	Must support 2X2 multiple-input multiple-output (MIMO) with TWO spatial streams

CT2WS2	wireless Standard	Must support simultaneous 802.11n on both the 2.4 GHz and 5 GHz radios and 802.11ac on 5ghz .
CT2WS3	wireless Standard	Must support data rates unto 800 Mbps on 5Ghz radio and 280 mbps on 2.4Ghz radio.
CT2WS4	wireless Standard	Must support 40 MHz and 80 MHz wide channels in 5 GHz.
CT2WS5	wireless Standard	Must support unto 25 dbm of transmit power in both 2.4Ghz and 5Ghz radios.
CT2RF1	RF	The Wireless AP should have the technology to improve downlink performance.
CT2RF2	RF	The AP shall be able to load-balance between 2.4Ghz and 5Ghz band.
CT2RF3	RF	Must have -90dB to -100B or better Receiver Sensitivity.
CT2RF4	RF	Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization
CT2RF6	RF	Should support configurable carrier sense threshold
CT2M1	Mesh	The Wireless Backhaul shall operate in 5Ghz
CT2M2	Mesh	Support Encrypted and authenticated connectivity between all backhaul components
CT2M3	Mesh	Access point shall have wired uplink interfaces i.e. 1X10/100/1000BASE-T Ethernet
CT2R1	Roaming	Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.
CT2S1	Security	Must support Management Frame Protection.
CT2S2	Security	Should support locally-significant certificates on the APs using a Public Key Infrastructure (PKI) or preinstalled certs on AP for authentication
CT2S3	Security	Provision of Wireless IPS to filter malicious traffic
CT2E1	Encryption	Access Points must support a distributed encryption/decryption model.
CT2E2	Encryption	Access Points must support hardware or software based encryption
CT2M1	Monitoring	Must support the ability to serve clients or monitor the RF environment .
CT2M2	Monitoring	AP model proposed must be able to be both a client-serving AP or monitor- Intrusion Prevention services.
CT2F1	Flexibility:	Should support mesh capabilities for temporary connectivity in areas with no Ethernet cabling.
CT2F2	Flexibility:	should support QoS for voice over wireless.
CT2F3	Flexibility:	Must support Controller-based and standalone(autonomous) deployments
CT2F4	Flexibility:	Must support 16 WLANs per AP for SSID deployment flexibility.

CT2O1	Operational:	Must support telnet or SSH or console login to APs directly for troubleshooting flexibility.
CT2O2	Operational:	Must support automatic detection of dropped connection to controller,
CT2O3	Operational:	Must support automatic failover to secondary controller, upon detecting lost connection to controller
CT2O4	Operational:	Must support DHCP Option 82, defined in RFC 3046, including support for Sub-option 01 (Circuit-Id) and Sub-option 02 (Remote Id) fields.
CT2O5	Operational:	With Controller APs (from a data-plane plane perspective) must support: - Ethernet over GRE IPv6 tunnel - Automatic detection of failed tunnel termination, with configurable connection retry and timeout. - Automatic failover to secondary tunnel termination address.
CT2O6	Operational:	Support for basic AP monitoring statistics for each radio: Bytes Sent, Bytes Received, Packets Sent, Packets Received, Radio Channel Utilization, Noise.
CT2O7	Operational:	Must support data-plane split tunneling in which ACLs may be configured to enable a range of destination net blocks and/or IPs to bypass the data-plane tunnel and be bridged on the wired interface.
CT2P1	Power:	Must support Power over Ethernet/PoE+/UPoE and AC .
CT2Q1	Quality of Service:	shall have the support of 802.11e and WMM
CT2Q2	Quality of Service:	Should be Wi-Fi Alliance certified and WPC Approved and ETA Certified
CT2Q3	Quality of Service:	Must support QoS to prioritize video ,voice and Data traffic
CT2EES1	Environmental and Electrical Specifications	Must support QoS and Video Call Admission Control capabilities.
CT2EES2	Environmental and Electrical Specifications	Access point shall support powering from POE/PoE+/UPoE and AC.
CT2EES3	Environmental and Electrical Specifications	Access point shall support pole, wall, and roof mounting options.
CT2EES4	Environmental and Electrical Specifications	Geographic orientation flexibility – tilt angle for pole, wall, and roof mounting units
CT2EES5	Environmental and Electrical Specifications	The equipment shall support up to 100 MPH sustained winds & 140 MPH wind gusts.
CT2EES6	Environmental and Electrical Specifications	The Access point shall be IP67 certified.

CT2EES7	Environmental and Electrical Specifications	The Access point shall be rated for operation over an ambient temperature range of 0C to +60 C

3. Category 3 Access Point:

Reference	Parameters	Technical specification
CT3HW1	Hardware	Must have a robust design for durability, without visible vents
CT3HW2	Hardware	Access Points proposed must include radios for both 2.4 GHz and 5 GHz.
CT3HW3	Hardware	Must include dual band antennas to support both the 2.4GHz and 5GHz operations simultaneously.
CT3HW4	Hardware	Proposed access point shall support MDO(Mobile Data offload)
CT3HW5	Hardware	Mounting kit should be standard which shall be used for mounting access point
CT3HW6	Hardware	Must Support operating Temperature of 0C to +40 C
CT3HW7	Hardware	Must support operating humidity of 10 to 90% (Non Condensing)
CT3WS1	wireless Standard	Must support 3x3 multiple-input multiple-output (MIMO) with three spatial streams
CT3WS2	wireless Standard	Must support simultaneous 802.11n on both the 2.4 GHz and 5 GHz radios and 802.11ac on 5ghz .
CT3WS3	wireless Standard	Must support data rates unto 1.3 gbps Mbps on 5Ghz radio and 400 mbps on 2.4Ghz radio.
CT3WS4	wireless Standard	Must support 80 MHz wide channels in 5 GHz.
CT3WS5	wireless Standard	Must support unto 22dbm of transmit power or better in both 2.4Ghz radios.
CT3S1	Security	Must support Management Frame Protection.
CT3S2	Security	Should support locally-significant certificates on the APs using a Public Key Infrastructure (PKI) or preinstalled certs on AP for authentication
CT3S3	Security	Provision of Wireless IPS to filter malicious traffic
CT3E1	Encryption	Access Points must support a distributed encryption/decryption model.
CT3E2	Encryption	Access Points must support hardware or software based encryption
CT3M1	Monitoring	Must support the ability to serve clients and monitor the RF environment concurrently.
CT3M2	Mesh	Support Encrypted and authenticated connectivity between all backhaul components
CT3M3	Mesh	Access point shall have wired uplink interfaces i.e. 2X10/100/1000BASE-T Ethernet
CT3F1	Flexibility:	AP model proposed must be able to be both a client-serving AP and Parallely monitor- Intrusion Prevention services.

CT3F2	Flexibility:	Should support mesh capabilities for temporary connectivity in areas with no Ethernet cabling.
CT3F3	Flexibility:	Mesh support should support QoS for voice over wireless.
CT3F4	Flexibility:	Must support Controller-based and standalone(autonomous) deployments
CT3F5	Flexibility:	Must support 16 WLANs per AP for SSID deployment flexibility.
CT3O1	Operational:	Must support telnet or SSH or console login to APs directly for troubleshooting flexibility.
CT3O2	Operational:	Must support automatic detection of dropped connection to controller
CT3O3	Operational:	Must support automatic failover to secondary controller, upon detecting lost connection to controller
CT3O4	Operational:	Must support DHCP Option 82, defined in RFC 3046, including support for Sub-option 01 (Circuit-Id) and Sub-option 02 (Remote Id) fields.
CT3O5	Operational:	With Controller APs (from a data-plane plane perspective) must support: - Ethernet over GRE IPv6 tunnel - Automatic detection of failed tunnel termination, with configurable connection retry and timeout. - Automatic failover to secondary tunnel termination address.
CT3O6	Operational:	Support for basic AP monitoring statistics for each radio: Bytes Sent, Bytes Received, Packets Sent, Packets Received, Radio Channel Utilization, Noise.
CT3O7	Operational:	Must support data-plane split tunneling in which ACLs may be configured to enable a range of destination net blocks and/or IPs to bypass the data-plane tunnel and be bridged on the wired interface.
CT3P1	Power:	Must support Power over Ethernet and AC..
CT3Q1	Quality of Service:	shall have the support of 802.11e and WMM
CT3Q2	Quality of Service:	Should be WiFi Alliance certified and passpoint certified and WPC Approved and ETA Certified
CT3Q3	Quality of Service:	Must support Reliable Multicast Video to maintain video quality
CT3Q4	Quality of Service:	Must support QoS toprioritize video ,voice and Data traffic
CT3R1	RF	Wireless AP Should detect and classify non-Wi-Fi wireless transmissions.
CT3R3	RF	Should support configuring the access point as network connected sensor to access any network location covered by the access point to get real-time Spectrum analysis data.
CT3R4	RF	Must have -90 to 100 dB or better Receiver Sensitivity.
CT3R5	RF	Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization
CT3RF6	RF	Should support configurable carrier sense threshold

4. Category Access Point:

Reference	Parameters	Technical specification
CT4HW1	Hardware:	Access Points proposed must include radios for both 2.4 GHz and 5 GHz.
CT4HW2	Hardware:	Must include dual band antennas to support both the 2.4GHz and 5GHz operations simultaneously.
CT4HW3	Hardware:	Proposed access point shall support MDO(Mobile Data offload)
CT4HW4	Hardware:	Must support a variety of antenna options.
CT4HW5	Hardware:	Must have -90 to 100 dB or better Receiver Sensitivity.
CT4HW5	Hardware	Must support operating humidity of 5 to 95% (noncondensing)
CT4WS1	wireless standard	Must support 3x3 multiple-input multiple-output (MIMO) with three spatial streams
CT4WS2	wireless standard	Must support simultaneous 802.11n on both the 2.4 GHz and 5 GHz radios and 802.11ac on 5ghz .
CT4WS3	wireless standard	Must support data rates unto 1.3 gbps Mbps on 5Ghz radio and 400 mbps on 2.4Ghz radio.
CT4WS4	wireless standard	Must support 80 MHz wide channels in 5 GHz.
CT4WS5	wireless standard	Must support unto 25 dbm of transmit power in both 2.4Ghz radios and 5 Mhz Radios
CT4WS6	wireless standard	Access point should support selective beamforming feature to improve performance of legacy 802.11abg clients.
CT4RF1	RF	The Wireless AP should have the technology to improve downlink performance
CT4RF2	RF	The AP shall be able to load-balance between 2.4Ghz and 5Ghz band.
CT4RF3	RF	Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization
CT4RF4	RF	Should support configurable carrier sense threshold
CT4R1	Roaming	Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.
CT4S1	Security	Must support Management Frame Protection.
CT4S2	Security	Should support locally-significant certificates on the APs using a Public Key Infrastructure (PKI) or preinstalled certs on AP for authentication
CT4S3	Security	Provision of Wireless IPS to filter malicious traffic
CT4E1	Encryption	Access Points must support a distributed encryption/decryption model.
CT4E2	Encryption	Access Points must support hardware or software based encryption
CT4M1	Monitoring	Must support the ability to serve clients and monitor the RF environment concurrently.
CT4M2	Monitoring	AP model proposed must be able to be both a client-serving AP and Parallely monitor- Intrusion Prevention services.

CT4F1	Flexibility:	Should support mesh capabilities for temporary connectivity in areas with no Ethernet cabling.
CT4F2	Flexibility:	should support QoS for voice over wireless.
CT4F3	Flexibility:	Must support Controller-based and standalone(autonomous) deployments
CT4F4	Flexibility:	Must support 16 WLANs per AP for SSID deployment flexibility.
CT4O1	Operational:	Must support telnet or SSH or console login to APs directly for troubleshooting flexibility.
CT4O2	Operational:	Must support automatic detection of dropped connection to controller
CT4O3	Operational:	Must support automatic failover to secondary controller, upon detecting lost connection to controller
CT4O4	Operational:	Must support DHCP Option 82, defined in RFC 3046, including support for Sub-option 01 (Circuit-Id) and Sub-option 02 (Remote Id) fields.
CT4O5	Operational:	With Controller APs (from a data-plane plane perspective) must support: - Ethernet over GRE IPv6 tunnel - Automatic detection of failed tunnel termination, with configurable connection retry and timeout. - Automatic failover to secondary tunnel termination address.
CT4O6	Operational:	Support for basic AP monitoring statistics for each radio: Bytes Sent, Bytes Received, Packets Sent, Packets Received, Radio Channel Utilization, Noise.
CT4O7	Operational:	Must support data-plane split tunneling in which ACLs may be configured to enable a range of destination net blocks and/or IPs to bypass the data-plane tunnel and be bridged on the wired interface.
CT4P1	Power:	Must support Power over Ethernet and AC
CT4Q1	Quality of Service:	shall have the support of 802.11e and WMM
CT4Q2	Quality of Service:	Should have Wi-Fi Alliance Certification and passpoint certified
CT4Q3	Quality of Service:	Must support Reliable Multicast Video to maintain video quality
CT4Q4	Quality of Service:	Must support QoS to prioritize video ,voice and Data traffic
CT4Q1	Mesh	The Wireless Backhaul shall operate in 5Ghz
CT4Q2	Mesh	Support Encrypted and authenticated connectivity between all backhaul components
CT4Q3	Mesh	Access point shall have wired uplink interfaces 2X10/100/1000BASE-T Ethernet
CT4EES1	Environmental and Electrical Specifications	Access point shall support powering from AC and POE/PoE+/UPoE.
CT4EES2	Environmental and Electrical	Access point shall support POE/PoE+/UPoE

	Specifications	
CT4EES3	Environmental and Electrical Specifications	Access point shall support pole, wall, and roof mounting options.
CT4EES4	Environmental and Electrical Specifications	Geographic orientation flexibility – tilt angle for pole, wall, and roof mounting units
CT4EES5	Environmental and Electrical Specifications	The equipment shall support up to 100 MPH sustained winds & 140 MPH wind gusts.
CT4EES6	Environmental and Electrical Specifications	The Access point shall be IP67 certified.
CT4EES7	Environmental and Electrical Specifications	The Access point shall be rated for operation over an ambient temperature range of 0C to 60 C
CT4EES8	Environmental and Electrical Specifications	Power consumption shall be less than 120 Watts meeting all safety specifications.
CT4EES9	Environmental and Electrical Specifications	Should Support Surge Protection on Line Earth, Power Inputs and Ethernet Ports to meet the requirement at High Voltage Transmission Line running across the Railway Platform. Must comply to all Rail Certifications not limiting to EN61000-4-2 Level 4 Contact / Level 3 Air ESD Immunity EN61000-4-5 Level 1 & 2 AC Surge Immunity EN61000-4-3 Level 4 EMC Immunity

Specification of Cloud/Appliance based Wireless Controller:

The below mentioned parameters are minimum specifications of the controller. Bidders has to propose Cloud/Appliance based Wireless Controller to meet the requirement as per the tender without any cost Implication for Railtel.

Reference	Parameters	Technical specification
WCHW1	Hardware and Standards	Must be compliant with IEEE CAPWAP or equivalent for controller-based WLANs.
WCHW2	Hardware and Standards	Controller should support 5000 access points from Day 1 from single chassis. If any OEM/Bidder can't provide WLAN controller to support 5000 AP in 2U form factor, multiple stackable controllers must be proposed from Day One from single chassis of minimum 2000 Access Point. Proposed controller should support 1+1/N+1 redundancy from the day one. The solution should be scalable to support 20000 or more APs. The cloud bases solution should be implemented in Railtel Data Centre
WCHW3	Hardware and Standards	Controller must have at least 4 x 10Gbps of uplink interfaces.
WCHW4	Hardware and Standards	Controller shall support 30000 concurrent sessions from a single chassis
WCHW5	Hardware and	WLAN controller shall support Mobile data offload as a feature

	Standards	
WCC1	Compatibility	Must not require a separate controller for Wireless Intrusion Prevention Access Points.
WCHA1	High Availability	Must support both 1+1 and N+1 redundancy models.
WCHA2	High Availability	Must have feature for stateful recovery without re-authentication of the client in the event of LAN and WLAN infrastructure disruption to deliver a non-stop client session
WCHA3	High Availability	Must support internal redundant power supplies.
WCRF1	RF Management	Must support an ability to dynamically adjust channel and power settings based on the RF environment.
WCRF2	RF Management	Radio coverage algorithm must allow adjacent APs to operate on different channels, in order to maximize available bandwidth and avoid interference
WCRF3	RF Management	Must have Automatic 802.11 interference detection, identification, classification, and mitigation.
WCRF4	RF Management	Must support coverage whole detection and correction
WCRF5	RF Management	Must support RF Management with 20/40/80 MHz channels with 802.11a/b/g/n/ac
WCIP1	IPv6 features	WLC should support L2 and L3 roaming of IPv6 clients
WCIP2	IPv6 features	WLC should support Guest-access functionality for IPv6 clients
WCP1	Performance:	Controller performance must remain the same if encryption is on or off for wireless SSIDs except the throughput processing of the controller.
WCS1	Security:	Should adhere to the strictest level of security standards, including 802.11i Wi-Fi Protected Access 2 (WPA2), WPA, Wired Equivalent Privacy (WEP), 802.1X with multiple Extensible Authentication Protocol (EAP) types, including Protected EAP (PEAP), EAP with Transport Layer Security (EAP-TLS), EAP with Tunnelled TLS (EAP-TTLS)
WCS2	Security:	Should support Management frame protection for the authentication of 802.11 management frames by the wireless network infrastructure.
WCS3	Security:	The Controller should support a capability to shun / block WLAN client in collaboration with wired IPS on detecting malicious client traffic.
WCS4	Security:	Controller should have rogue AP detection, classification and automatic containment feature
WCS5	Security:	Controller should be able to detect attacks like Broadcast deauthentication, NULL probe, from day one for all access points
WCS6	Security:	Controller should have profiling of devices based on protocols like HTTP, DHCP and more to identify the end devices on the network
WCG1	Guest Wireless	Must support internal and external web authentication.

WCF1	Functionality	Must be able to set a maximum per-user bandwidth limit on a per-SSID basis.
WCF2	Functionality	Must support user load balancing across Access Points.
WCF3	Functionality	Controller must provide Mesh capability for Mesh supported AP.
WCM1	Monitoring	Must be able to use APs to monitor for Intrusion Prevention Services
WCR1	Roaming:	Must support client roaming across controllers separated by a layer 3 routed boundary.
WCR2	Roaming:	Solution proposed must support clients roaming across at least 500 APs.
WCO1	Operational:	Must support AP over-the-air packet capture for export to a tool such as Wire shark.
WCO2	Operational:	Should be able to classify different types of interference
WCO3	Operational:	Should provide a snapshot of air quality in terms of the performance and impact of interference on the wireless network identifying the problem areas.
WCO4	Operational:	Should provide real-time charts showing interferers per access point, on a per-radio, per-channel basis.
WCO5	Operational:	Should support encrypted mechanism to securely upload/download software images to and from wireless controllers
WCO6	Operational:	Must support Ethernet over GRE IPv4 tunnel to northbound gateway
WCO7	Operational:	Should support Ethernet over GRE IPv6 tunnel to northbound gateway
WCO8	Operational:	Must support automatic detection of failed tunnel termination, with configurable connection retry and timeout
WCO9	Operational:	Must support automatic failover to secondary tunnel termination address.
WCO10	Operational:	Must support controller-based configuration of Ethernet over GRE tunnel termination
WCO11	Operational:	must be wifi passpoint 2 complaint
WCO12	Operational:	System shall support various modes of operations like Tunnel Mode and local Breakout on the Same AP
WCO13	Operational:	Must support configuration of data-plane split tunneling by enabling specific destination IP addresses and net blocks to bypass the data-plane tunnel and be bridged on the wired interface
WCO14	Operational:	Shall Support WAG functionality for WiFi offload
WCO15	Operational:	shall support API's for NB Integration with CNMS
WCO16	Operational:	System shall support Reporting functionality without any external server
WCQ1	QOS:	Must support 802.11e (WMM)
WCQ2	QOS:	Shall able to prioritize all traffic such as (Data ,voice and video)
WCQ3	QOS:	Controller shall integrate with existing firewall and deep packet inspection

WCQ4	QOS:	Should have rate limiting per user and per SSID basis for encrypted tunnel mode
WCQ5	QOS:	To deliver optimal bandwidth usage, reliable multicast must use single session between AP and Wireless Controller.

10. All other Terms & conditions will remain same.

.

(A.K.Sablania)
Group General Manager/DNM