Request for Proposal (RFP)
America's Cup 2017 Telecommunications Requirements (Wi-Fi Deliverables)

This document is issued by WEDCo, with insight & support from ACBDA Telecommunications Team.

In collaboration WEDCo, the ACBDA Telecommunications Team, are issuing a Wi-Fi RFP for an exclusive Wi-Fi solution covering the WEDCo area (as outlined in the attached document) which will start 1 February 2017 with a 5 year contract including a revenue sharing model or other benefit for WEDCo and will be used for the Americas Cup 19th May through 4th July 2017.

Definitions:
"WEDCo" – West End Development Corporation
"ACBDA" – Americas Cup BDA Telecommunications Team
"The Team" - WEDCo & ACBDA

Decision Authority
WEDCo will be the final decision making authority & signature authority for the contract.

ACBDA Telecom Team will provide input to create the RFP, provide Americas Cup capacity requirements and deliver a recommendation to WEDCo.

1 Executive Summary

1.1 "The Team", is issuing an RFP to all appropriate vendors in Bermuda to bid on the Wi-Fi communications requirements for Dockyard including the "Cross Island" (America's Cup Village) from 1 February 2017 for a 5 year period with the option, by WEDCo, to extend for an additional 5 years.

1.2 The Team is looking for innovation options for the delivery of Wi-Fi that provides a benefit to WEDCo, with revenue sharing options or other service benefit options during the contract period. For the Americas cup and the service required for Cross Island this element could be a temporary build solution – that is then used elsewhere – or a permanent solution depending on the eventual use of Cross Island which is still to be determined.

1.3 The key Americas Cup events are planned for 19th May through 4th July 2017 and the Wi-Fi services on the "Cross Island" (America's Cup Village) and other specifically identified event areas are to be free of charge during this period.

1.4 The following outlines the process that will be followed by "The Team" to seek & review proposals from potential vendors

2 Submission Deadline

2.1 Vendor proposals must be submitted by 30 September 2016 for the Wi-Fi deliverables. See summary of key dates in section 15.

3 Submission Delivery

3.1 Vendors may deliver submissions by e-mail to:

Fiona@fionabeck.me and copied to Kent Bascome Kbascome@wedco.bm

3.2 Proposals submitted via e-mail must have **"The Team RFP Response"** in the subject line and must be submitted with a **read receipt** notifier activated. The response must be in unlocked Microsoft word and/or excel format.

3.3 All submissions become the property of "The Team" and will not be returned. All conditions contained in the RFP are considered accepted by the vendor in any information submitted.

3.4 All information submitted with the RFP will be kept confidential and access will be only by WEDCo, ACBDA, ACBDA Telecommunication team's reviewing the RFP. "The Team" is not obliged to award orders or contracts to vendors based on the information received.

4 Vendor Submissions

4.1 The Wi-Fi solution will start 1 February 2017 with a 5 year commitment and an option for an additional 5 years. This should include a yearly capacity review and increase as appropriate and also a 3 year equipment refresh as required.

4.2 The services to be delivered are detailed in the attachment "Wi-Fi Deliverables" document

4.3 The Wi-Fi services for the "Cross Island" (America's Cup Village) included in the "Wi-Fi Deliverables" document are part of the overall Bermuda commitment for hosting the America's Cup. These services are to be free of charge during the period of events within the America's cup 2017 calendar – from 19th May through 4th July 2017. In addition, the Wi-Fi services are to be free for any future America's Cup events which occur 3+ years apart.

4.4 Submissions may be from individual vendors or multi-vendor consortiums. In the case of vendor partnerships, one vendor must be clearly identified as the primary contractor, with all others being indicated as sub-contractors. Primary Vendor's must be Bermuda Registered Companies & hold an ICOL (Integrated Communications Operating License). Please note if you are not an ICOL holder you are able to partner with an ICOL holder and your bid would need to be structured such that the Telecoms piece is managed by the license holder with the other contracting party holding the prime relationship with ACBDA for delivery of the tender proposal.

4.5 Submissions must include the following information:

4.5.1 ***Proposed Services -*** A description of the proposed services that will meet the requirements set out in the attachment entitled "Wi-Fi Deliverables". The description should set out the functions and features of the services. Changes to your existing services which require Government approval should be highlighted with cut off dates after which services will not be possible to be provided. The description should also set out the proposed approach to implementation of services as appropriate.

4.5.2 ***Company Information -*** Including vendor qualifications and experience as well as background information on the personnel proposed to work & support the services.

4.5.3 ***High-level Services Project Plan -*** This will show how the vendor proposes to approach the project and the major milestones to meet & exceed the Wi-Fi Deliverables.

4.5.4 ***Change of control process –*** Document the preferred change of control process for easy tracking and documentation trail as the requirements emerge.

4.5.5 ***Responsibilities of the ACBDA Team –*** Run a transparent process and provide information as required to the vendors to meet the submission date.

4.5.6 ***Summary of Proposal –*** Include an executive one page summary

5 Pre-submission Information

5.1 All prospective vendors will be provided with this documentation and the opportunity to submit written inquiries to "The Team". As appropriate, such inquiries will be published, without identifying the source, along with response to all vendors.

5.2 Inquiries regarding this request for proposal must be made by email, with "**The Team WiFi Deliverables Inquiry"** in the subject line, by 20 September 2016 to Fiona@fionabeck.me and copied to Kent Bascome Kbascome@wedco.bm.

6 Vendor Responsibility

6.1 It is the vendor's responsibility to ensure its complete understanding of the requirements and instructions specified by "The Team". In the event that clarification is required vendors should submit written inquiries as described in paragraph 5.2 above.

7 Amendments

7.1 At any time prior to the close of the RFP, "The Team" may alter, amend, delete or add to, in whole or in part, any terms or provisions of this RFP. "The Team" will email any changes to all vendors who received the original RFP.

8 Evaluation Process

8.1 The proposals submitted to "The Team" will be evaluated and the vendors will be offered a meeting with the "The Team" to present their submissions and answer qualification questions, which may result in the award of a contract. The only information that will then be released is the name of the successful vendor.

8.2 It is anticipated that potential vendor will be selected by 20 September 2016.

8.3 The criteria for selection will be based on the following:

- Robust technology platform saleable network, frequency management (20%)
- Quality of service and proactive network management, Software defined network capabilities (20%)
- Experienced vendor with proven track record, project management capabilities (20%)

- Proposal value proposition and Revenue sharing model or benefit derived to WEDCo(30%) Note the revenue sharing model will be based on Gross Revenue including all types of revenue for example subscription and advertising revenue
- Support for Bermuda and legacy nature of solution (10%).

Please note for the RFP it is intended that the provider cover all costs (capex and operating, local loop etc) and these will be borne by the operator in return for rights to operate and charge (Americas Cup public areas aside which will be free during the event) in the greater dockyard area over the contract period. The cost of doing so will be recovered by the operator by way of the revenue sharing arrangements.

9 Negotiations

9.1 WEDCo reserves the right to enter into discussions or to negotiate with a vendor as it sees fit, or with another vendor or vendors concurrently. In no event will Wedco be required to enter into discussions or negotiations on similar or other terms or offer any modified terms to any other vendor prior to entering into a binding contract. "The Team" shall incur no liability to any vendor as a result of these discussions, negotiations or modifications.

10 Acceptance and Authority to cancel this RFP

10.1 "The Team" will not be obliged to accept the lowest price or any of the proposals submitted. Each vendor acknowledges and agrees that "The Team" will have no liability or obligation to any vendor, except to the party, if any, awarded a contract by "The Team" in its sole discretion and "The Team" shall be fully and forever released and discharged of all liability and obligation in connection with this Request for Proposal (RFP). "The Team" will not make public the vendor submissions and reserves the right to cancel this RFP without any obligation or reimbursement to vendors.

11 References

11.1 Before awarding any contract "The Team" reserves the right to require the vendor to submit such evidence of qualifications as it may deem appropriate. This evidence may be concerning financial, technical and other qualifications as well as the relevant experience and skills of the Vendor.

12 Service Delivery

12.1 The services are considered delivered when running and signed off by WEDCo.

13 General

13.1 All proposals will be considered final. No additions, deletions, corrections or adjustments will be accepted after the time stated above.

13.2 Proposals received after the designated time of receipt will be considered as "NO BID" and "VOID". The time stamp for proposals submitted electronically will be that of the read receipt you receive from ACBDA Chair email. It is the vendor's responsibility to allow sufficient time for electronic transmission and delivery, especially in the case of large files.

13.3 Upon awarding and acceptance of a contract for services WEDCo will issue an award letter.

14 The Team

WEDCo	Andrew Dias
	Kent Bascome
Chair:	Fiona Beck
Members:	Anthony Briscoe
	Michael Branco
	Kim Perdikou
	Aaron Smith
	Michael Wells

15 Summary of Key Dates — Wi-Fi Deliverables

Publish Request for Proposal	13-Sep-16
Final date for questions	20-Sep-16
Vendor proposals submitted	30-Sep-16
Vendor Presentation	10-Oct-16
Preferred Vendor recommendation	17-Oct-16
Vendor selection	31-Oct-16

16 Attachments

1. Wedco Area and Statistics for planning purposes
2. Wi-Fi Deliverables
3. Coverage Map

WEDCo Area & Statistics – Attachment 1

Dockyard and Cross Island (the America's Cup Village)

Cruise ships

- Off season (Nov – March) ~ 4k -5K visitors
- Season (April – Oct) ~ 8k - 12K visitors

Maximum 20K visitors (during America's cup with cruise ship visitors)

Potential opportunities:

- Dockyard Commercial – approx. 50 businesses
- Pier 4 resident marina tenants

Wi-Fi Deliverables - Attachment 2

Overall Services

The overall Wi-Fi services must be capable, at the specified services levels, to deliver the following services:

- Wi-Fi Access bandwidth for WEDCo to set up wireless cameras for Video surveillance within the Wi-Fi coverage area
- Wi-Fi Internet Subscription Services for visitors to Dockyard
- Provide a Wi-Fi Advertising Services delivery as agreed during the RFP process
- Maintain all Wi-Fi infrastructure including access points and Splash Page (Other than the splash page provided (aka required to be used) by the America's Cup for the Free Wi-Fi Period)
- Procure all local loops, infrastructure required to deliver an end to end service for WEDCo (As a pass through cost to WEDCo)

Detailed Specifications

WEDCO in conjunction with America's Cup Bermuda are looking for an experienced and innovative telecom provider to propose, implement and manage a service provider class wireless network (802.11) in Dockyard to service the following target users:

- Tourists (visiting via cruise ship)
- Residents of Bermuda (visiting the campus)
- Tenants of the WEDCO properties (corporate grade access service)
- America's Cup corporate users
- America's Cup audiences (May / June 2017)
- America's Cup fans in Fanzone (Cross Island)

It should be noted that the successful provider will be required to provide free public wifi in Dockyard Americas Cup designated event areas and Cross Island during the dates of America's Cup 2017 (May 24th, 2017 → June 30th, 2017) and in any subsequent Americas Cup future event should one occur during the contract period.

Evaluation criteria will be done by WEDCO in conjunction with the America's Cup Telecom Committee, with a focus on the following key items:

- Robust technology platform
- Scalable wired and wireless network
- Frequency management
- Quality of service and proactive network management

- Software Defined Network capabilities
- Experienced vendor with proven track record
- Strong project management capabilities
- Ability to operate the network profitability for all stakeholders

The bidder has the scope to provide an innovative proposal that addresses the requirements listed in this document but bidders are welcome to make suggestions to tweak or expand on the proposal to make the offering more attractive.

Based on experience from previous America's Cup events in Bermuda and overseas, the following areas should be considered in the proposal.

Frequency Audit

The proposal should include at least two frequency audits to help plan the build of the network and monitor it during critical times such as the Americas Cup Event.

Service Provider Network

A service provider network is the preferred architecture to allow for handling of public Wi-Fi and corporate Wi-Fi users with offloading capability and peering with cellular providers.

Payment Engine / Paywall

The system should support multi-tier paywall with a payment engine supported with local banks.

Cache

The system should support an on-island cache mechanism to keep frequently accessed objects nearby on the network to help with network performance and user experience.

Legacy

The proposed system should focus on the long term nature of the partnership and offer Dockyard a legacy network beyond the immediate needs of AC35.

Pen Test / Security

The provider should schedule penetration tests at regular intervals (i.e. 4 x year) to test the vulnerabilities of the network and ensure remediation is part of this proactive process.

Video Cameras

The network should support a number of different types of traffic, including video cameras and VOIP, managed through VLANS and QoS, or other industry standard methods. Suggestions on compatible video cameras and security system are welcomed.

Redundancy

The WLAN should meet the requirements of redundancy listed below, but the provider should also demonstrate an architecture that utilizes local loop and off-island redundancy in a cost effective manner.

Bandwidth Shaping

At a high level the system should allow for bandwidth shaping based on user profiles and providers should demonstrate if their system can support a SDN architecture.

Project Management

It is important for the provider to not only demonstrate their superiority in technology but also in their project management capabilities utilizing well defined plans, clear communication plans and robust execution of the plans.

Monitoring

The provider should speak to the monitoring capabilities in the proposed network, demonstrating what monitoring tools are being utilized, proactive alerting and resolution, managed under a NOC. The provider should also show the table related to their SLA and response times, including the escalation matrix. The SLA should also show the Outage Penalty calculations.

Campus Fiber Loop

As part of the WLAN backbone, WEDCO will provide conduit throughout Dockyard and Cross Island to allow for the provider to price and propose laying the fiber loop backbone required for this network.

Core Network Design

The provider will show the core network design (physical and logical), including on-campus, back haul, redundant POP, off-island connections and overseas POPs with connectivity.

Sample Implementation Plan

The provider will show a sample implementation plan and 5-year maintenance plan for the proposed network.

Financials

The provider will provide all financials including, but not limited to:

- All local loop costs
- Bandwidth costs
- Project costs
- Profit sharing model (or other Benefit to WEDco)
- Upgrade & maintenance cost estimates for 5 years

Allowing for WEDCO to fully understand all financials involved with this undertaking.

Please note that for the RFP it is intended that the provider cover all costs (capex and operating, local loop etc) and these will be borne by the operator in return for rights to operate and charge (Americas Cup public areas aside which will be free during the event) in the greater dockyard area over the contract period. The cost of doing so will be recovered by the operator by way of the revenue sharing arrangements.

Capacity

The WLAN should have the ability to service all tenants and tourists during the regular season and scale up to 10,000 people for Americas Cup specific events.

ICOL Holder

The provider shall provide proof of an active ICOL for the duration of the contract.

Performance Review

The provider will outline a schedule for an annual performance review of the network, highlighting key metrics and will be contracted to manage the failure to meet certain thresholds, with clauses for service credits and termination of contract in extreme cases.

The following is an outline of the areas that will be reviewed in detail with the preferred vendor. For your initial bid you should describe at a high level key matters relating to subject areas below.

1. Architecture Overview and System Technology

1. Provide a brief overview of the wireless system architecture and elements (i.e., is it an integrated system with a centralized intelligent device or a series of autonomous access points, or APs?)

2. Does the system allow Network Management to designate the way data is forwarded (either centralized at the controller, or distributed at the AP) for different applications and types of traffic?

3. Can traffic be restricted, permitted or prioritized by user, group of users, SSID, application, source/destination IP, protocol and CoS?

4. Please describe any aspects of the architecture that help the network scale on the following attributes:
    - Throughput
    - User and system control
    - Management
    - Increasing total traffic
5. What kind of antennas do the APs support?
6. Do the outdoor APs support the same functionality and features as the indoor APs? If not, what are the limitations of the outdoor APs?
7. Do all APs (indoor and outdoor) have mesh technology to link to each other wirelessly?
8. What kind of antenna options are available with the outdoor AP?
9. What are the environmental specifications for the outdoor AP?

2. Planning and Design

1. To what extent are site surveys required both for initial installation and for when a site plan is changed?
2. Does the system allow the integration of CAD drawings for site plans (e.g. DXF, DWG file formats) to spatially determine the number and placement of APs?
3. How do the planning process and tools determine the number and placement of APs to deploy? Describe how bandwidth requirements are incorporated into this design. Please highlight where processes are automated.
4. Describe how "what-if" scenario planning is handled. Describe the ability to handle network designs requiring more or less bandwidth capacity, various radio technologies, and differences in site plan or other potential RF obstructions.
5. How do the planning process and tools determine the various APs' RF channel assignments, power levels and association rates? Please highlight where processes are automated.
6. How does the system help plan for redundancy?
7. We have a large and complex facility with many physical obstacles but we want to run voice over Wi-Fi. How does the system ensure seamless RF coverage in such an environment? Can the system validate the RF measurements from a physical site survey with the built-in virtual site survey?
8. If we plan to deploy our wireless LAN beyond a single campus. How can we scale security and services to our branch offices without creating a management problem?

3. Deployment and Configuration

1. It is critical to understand the deployment and configuration processes of the proposed system. In particular, the following questions seek to capture the costs to configure, deploy and maintain the wireless system, especially as needs evolve and the environment the WLAN serves changes.

2. Please describe how the system plan becomes incorporated (configured and deployed) into the actual equipment BOM. Please highlight where processes are automated.

3. What is the configuration needed on aggregation or edge switches and routers? Please detail.

4. Do your APs automatically configure themselves for optimal channel and transmit power when they become operational?

5. How does the system simplify the deployment of wireless services such as voice and security to all locations?

4. VLAN Support

1. How does the system support multiple VLANs over the air?

2. Does the WLAN system support 802.1X dynamic VLAN policies?

3. Does every VLAN have to be accessible on every subnet supporting an AP for the WLAN?

4. Does the system allow the network manager to limit multicast traffic in the WLAN?

5. What is the maximum number of VLANs, APs and users that can be supported in a single WLAN controller? In a system of controllers?

5. Security – AAA, Encryption, Traffic Isolation

A significant concern is the breadth of security measures supported by the proposed WLAN system. The following questions are designed to determine standards adherence, range of security protocols supported and future-proofing of the system.

1. What methods of authentication are supported?

2. Does the system support web-based AAA?

3. Which EAP protocols are supported?

4. Can users associated with third-party APs be authenticated?

5. Can the controller act as an AAA server for its wireless clients?

6. Can EAP processing be offloaded from the AAA server to the controller?

7. What encryption methods does the system support?

8. Where does the system store user and network data? Is there any data locally stored on the APs? Is direct access to the APs supported?

9. Does the system support per-user in-bound and out-bound extended access control lists (ACLs)? Per-port ACLs? Per-VLAN ACLs?

10. Does the system include a utility for a non-technical designee (e.g. receptionist) to supply temporary credentials to guests? If so, does the provisioning of the credentials affect the controller's configuration?

11. Does the system support endpoint assurance to protect the corporate network from a compromised laptop or other mobile device?

12. Does the system support Microsoft Network Access Protection for endpoint assurance?

13. Does the system enable scalability through distributed cryptography, or does it require centralized encryption of wireless data at the controller?

14. Is any sensitive data stored locally on the APs? If so, what type of data is stored there?

6. Intrusion Detection and Countermeasures

One goal of WLAN deployment is to use the system as a mechanism for detecting and locating rogue access points and users. The following questions are aimed at understanding how the proposed system aids in this critical function.

1. Does your WLAN support wireless intrusion detection/prevention (WIDS/WIPS) or does it require a separate overlay for WIDS/WIPS?

2. Does your solution provide for remediation against rogue access points and denial of service attacks?

3. Does your WIDS/WIPS have integrated configuration and management?

4. Do intrusion alarms automatically roll up in your WLAN management console?

5. Does your management console provide a single consolidated view of intrusion alarms and WLAN status?

6. Do your WLAN and WIDS/WIPS leverage common hardware for APs and intrusion sensors?

7. Does the system perform rogue detection automatically?

8. What countermeasures are employed against rogues that are found?

9. Does the system send alerts when rogues are detected?

10. What types of management logs and traps for rogue activity can be shown?

7. Roaming

1. How does the system support roaming between APs or between WLAN controller when the APs or controllers reside on different subnets?

2. Can users maintain the same IP address as they roam?

3. Does a roaming user need to re-authenticate or re-login?

4. Does the user's subnet attributes (VLAN, ACLs, route policies) follow the user as s/he roams?

5. Does the system support any mechanisms to control where users can physically roam throughout the WLAN infrastructure?

6. For large installations, can the system perform fast-roaming (802.11i) between controllers?

8. Voice over Wireless LAN

For many organizations, there is a need to support both voice and data services over the same WLAN infrastructure. The following questions are designed to discover how the WLAN system supports voice.

1. How do your network management capabilities help plan for voice over wireless LAN (VoWLAN, voice over Wi-Fi)?

2. Describe the suitability of this architecture for supporting voice over wireless LAN. What is it about the system's architecture that may help voice service?

3. Does the system automatically calculate voice coverage and capacity requirements?

4. Does the system support 802.11e and related standards to preserve voice prioritization? If so, does it support:

   - WMM
   - WMM Powersave [U-APSD]
   - TSPEC?
   - CAC

5. Does the system enable seamless roaming between networks (e.g., FMC, Wi-Fi and cellular roaming)? If so, how?

6. Does the system support dual-mode handsets?

9. Location-Based Services

Our organization is interested in location-based tools that utilize the Wi-Fi infrastructure. The following questions are designed to understand how the system supports location-based services and applications.

1. As facility-wide deployments of WLANs become more common, new service possibilities are created, such as using Wi-Fi access points to track the physical location of Wi-Fi client devices and Wi-Fi tags. Describe how the WLAN system supports location-based services.

2. Can the wireless access points be used to track assets?

3. How many tags does the system support?

4. Does the system support choke point alerts?

5. Do you offer a separate location appliance?

6. If so, briefly describe the appliance, what location technology it employs, and its expected accuracy at different distances – e.g., accuracy at 1 meter, 3 meters, 10 meters.

10. System Capacity and Performance

A major concern is that the WLAN provide sufficient capacity for business-level application performance. The following questions will help in determining how the system helps IT design for performance vs. simple RF signal reach.

1. Does the system help IT design for capacity as well as coverage? Can it allow IT to set minimum or average bandwidth requirements per user?

2. Does the system support setup and enforcement of minimum association rates to improve system performance? Please detail.

3. Does the system support per-user QoS capabilities and prioritization via per-user queuing in the APs?

4. Does the system enable IT to control an AP's transmit power level via software? If so, is it automated, or does each AP need to be adjusted separately?

11. Management

A major concern is the ability to manage the air as a network resource. The following questions are critical to understanding the controls and performance of the proposed wireless system, and the ability to generate key user statistics.

1. Does the system use data from the planning process to manage and verify actual WLAN operations? If so, how often does it verify operations?

2. Can the management tool schedule reports for automatic generation? If so, how are the reports generated and delivered? Can they be automatically sent to the network manager via email?

3. What types of configuration and monitoring reports can be generated?

4. Does the system allow IT to force a user off the network?

5. Does the system allow IT to set up a user session timeout?

6. Does the system allow IT to track a user's AP associations, both current and historical?

7. Can the system monitor a user's bandwidth consumption, system performance, roaming path, and time on the system?

8. What information about bandwidth usage does the system track? Can it provide a breakdown by user? Can it provide a breakdown of any other groupings?

9. What type of reporting is available when rogues are detected?

10. Does the system tie to AAA accounting? Can the system enable departmental charge back for WLAN services? Please detail.

11. Does the system support exportation of management graphs and statistics files?

12. How many controllers/switches does your WLAN management solution support per server?

13. Does the system enable network-wide change management?

14. Does the system provide trend monitoring?

15. Does the system provide end-user customizable reports?

16. Does the system support the ability drill down to real-time and historical data?

17. Does the management system come in a software or hardware appliance?

18. Please detail the benefits of each option – hardware and software - if relevant.

12. Redundancy, Reliability and Resiliency

1. Does the system provide for redundancy? If so, describe briefly how the redundancy system works.

2. How much extra cost is required to provide redundancy. Please specify in terms of:

3. Additional capital costs for controllers. Specify the number of extra controllers that are recommended for full redundancy.

4. Additional capital costs for access points. Specify the number of extra access points that are recommended for full redundancy.

5. Specify the additional software licensing SKUs and license fees to fully enable all the redundancy features.

6. Redundancy Experience for End Users

    - How fast is the failover in the case of a network outage? Please specify in ms. (milliseconds)

    - What happens to data clients in the event of a failover?

    - How long is the delay before data service is restored?

    - What actions must the user take to re-obtain data service? (re-associate, re-authenticate, re-log in, etc)

    - What happens to voice clients in the event of a failover?

- Is the current voice session terminated?
- How long is the delay before voice service is restored?
- What actions must the user take to re-obtain voice service? (re-associate, re-authenticate, re-log in, redial the call, etc.)

7. What redundancy mechanisms are available in the AP?
8. Does the AP have two 10/100/1000 Mbps ports for redundant power?
9. Does the AP have two 10/100/1000 Mbps ports for redundant data?

13. Scalability and Technology Migration

A primary concern is the ability to scale and grow the wireless system easily over time, both in terms of the number of total users and in overall capacity. The following questions will help detail what tools are available to scale the proposed system.

1. What is the maximum number of BSSIDs supported by each AP?
2. Can traffic be encrypted in a distributed fashion by the APs or is all traffic required to pass through the controller?
3. Does the management application support centralized management of APs and controllers or does it require accessing each controller separately?
4. What is the maximum number of controllers that the management application can accommodate? What is the maximum number of APs?
5. Does the planning application support multiple buildings?
6. Does the planning facility compute optimal AP channel and power settings for buildings with multiple floors?
7. Does the management application monitor the wireless system enterprise-wide?
8. Are 40 MHz channels supported on the 5GHz band?
9. What is the MIMO configuration of the AP?
10. What is the maximum number of APs supported by the highest end controller? For a stackable system, provide the number of APs for each rack-mounted stackable. For a chassis/ blade system, provide the number for each blade.
11. For a stackable system, does the system support virtual (logical) stacking, or must the stackable units be physically connected to each other in the same rack?

14. Standards and Interoperability

Adherence to industry standards is critical in the wireless arena, especially since the environment will support a wide range of client types. The following questions will help detail the specifications the proposed system supports.

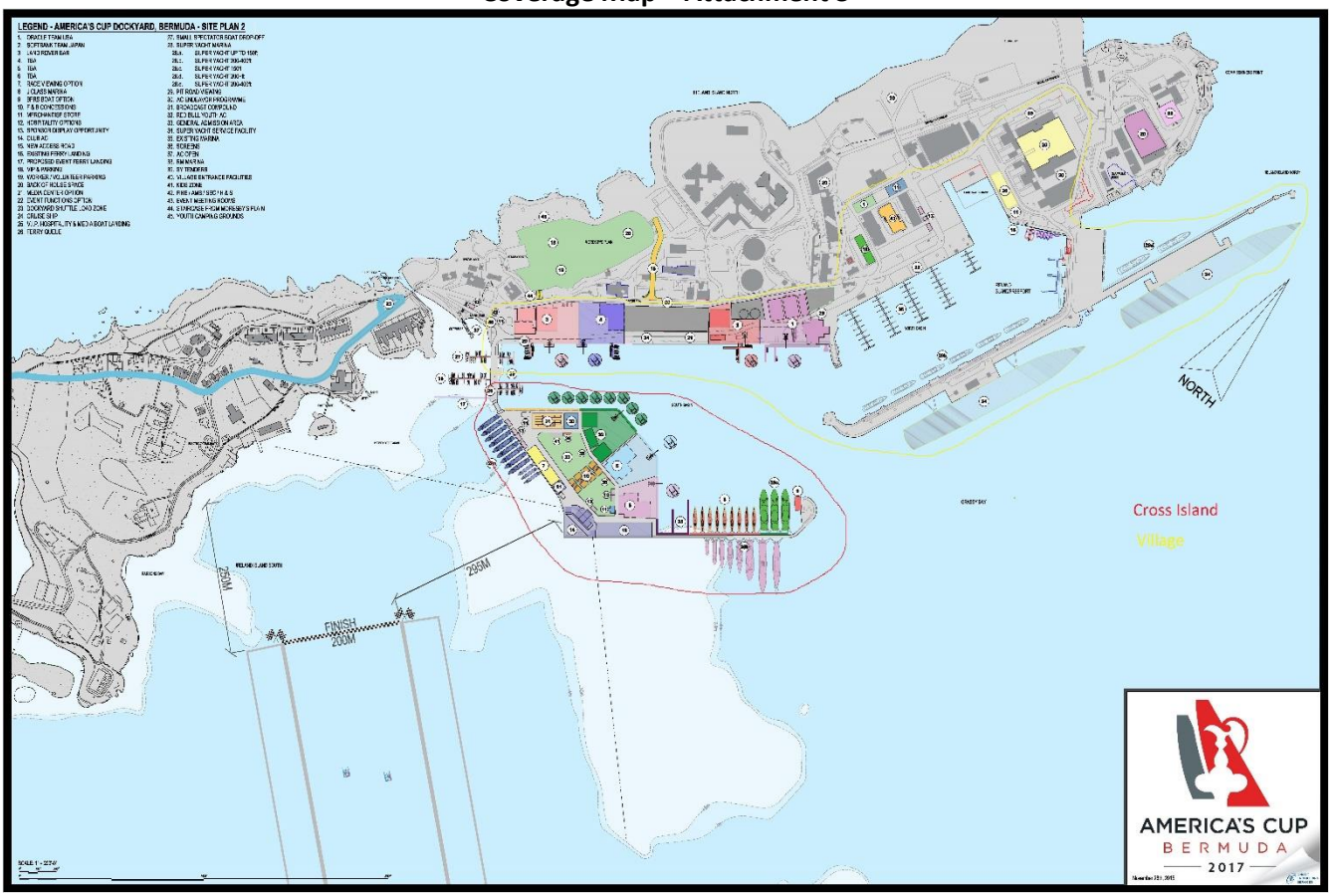
1. Is the system Wi-Fi certified?
    - If so, for what operations?
    - Is it Wi-Fi Certified for WPA and WPA2? (Wi-Fi Protected Access/2)
2. Do the APs support 802.11a/b/g?
3. Do the APs support 802.11n?
4. Do the APs support WPA with TKIP encryption?
5. Do the APs support WPA2 (802.11i) with AES encryption?
6. Do APs support standard 802.3af POE?
7. Do APs support pre-standard 802.3at POE?
8. Do the APs support 802.11i fast-roaming?
9. Does the wireless system support 802.1X?
10. Does the wireless system support 802.11d?
11. Does the wireless system support 802.11h?
12. Is multicast traffic supported? If so, how does the wireless system determine the data rate when serving many clients?

15. Granular Access Control

1. Describe briefly how the system determines the proper user authorizations.
2. Location Integration
    - Does the system integrate with an accurate location appliance to determine authorizations based on physical location? If so, briefly describe how the integration works.
    - If so, specify the name and model of location appliance that works with the system.
    - Specify the location accuracy of the location appliance that works with the system.
3. Can authorizations change based on reaching certain RADIUS accounting metrics, such as total traffic passed?

4. Can IT use the system to set access control rules for authorization? If so, can it set rules based on:
    - SSID?
    - User Name pattern (e.g. domain\username)?
    - User Type? (e.g., voice, data, video, guest)
    - Location? (physical location provided by location appliance)
5. RADIUS accounting metrics? (lifetime or session metrics)
6. What actions can the system perform against the matched conditions set by IT?
    - Can it change authorization attributes?
    - Can it connect and disconnect a user session?
7. In session updates. Does the system update authorization attributes on re-authentication only (next networking session) or can the system support in-session updates of authorization attributes based on the conditions and access control rules set by IT?
8. Specifically, can the system support in-session updates:
    - On client re-authentication?
    - On client RADIUS accounting start or interim updates?
    - On client roam to a new AP?
    - On location change?
9. Describe how and when the authorization rules are invoked. Can the system invoke authorization rules:
    - Automatically, upon meeting the conditions?
    - Scheduled to run at set times?
    - On-demand through the system GUI?
    - Through a web-based API?

Coverage Map – Attachment 3



Note Dockyard area starts at Cockburns Cut Bridge

Americas Cup Free Wi- Fi area Cross Island (circled in red) and yellow America Cup event areas 20 and 26.

Please note this village plan is still a working draft and subject to slight modifications.