Technical Bulletin: LAB Validation of PCI segmentation using profile names vs VLAN numbers.

1 ABOUT THIS DOCUMENT

This document is to serve as the basses for testing and evaluating the optimum configurations for Cisco and Aruba as it relates to AAA override and the PCI desired functionality.

1.1 DOCUMENT AUTHOR(S)

Name	Organization	Role
Michael Grimaldi	DTSS-Enterprise Wireless	Wi-Fi Architect
David Carrasquillo	DTSS–Enterprise Wireless	Wi-Fi Architect

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

1.3 DOCUMENT REVISION HISTORY

[redacted]		[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Contents

3 SUMMARY & PURPOSE

The purpose of this document is to provide a method for evaluating the optimum configuration of the desired PCI segmentation with two wireless vendors Cisco and HPE (Aruba) as well as two configurations Locally switched user data and centrally switched user data models. Each manufacture

NOTE: PCI segmentation is required and will be enforced by the use of RADIUS override commonly referred to as CoA (Change of Authority).

3.1 HOMOGENOUS NETWORK ENVIROMENT (SEAMLESS ROAMING)

During the initial implementations of the Crown / Disney Wi-Fi networks at the WDW Parks and Resorts a design decision was made to maintain a separation between the networks which is commonly referred to as the "Back of House" vs "Front of House" theory. Where the "Front" is considered Guest Facing and the "Back" is Cast Only areas. While on the surface this sounds very clean and advantages to providing the best possible solution to the end users, it has turned out to be the Achilles' heel of the networks. This is primarily due to the common overlapping of coverage areas. The "Front" and "Back" of houses are often only separated by a single drywall partition or less. Because of the close proximity the need to support layer 2 roaming between the networks has reached a critical mass. As we move to a more wireless oriented service model for guest facing and guest supporting technologies, we are compelled now to address the issue and have jointly agreed to pursue the techniques outlined in this document.

3.1.1 Network Security and Isolation

[redacted]

3.2 SPECTRUM SEPERATION

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

3.3 PCI SEGMENTATION

[redacted]

4 AUDIENCE

The intended audience for this document is for:

- Crown Management, Network Engineers and Architects
- ATOS Management, Network Engineers and Architects
- DTSS Management, Network Engineers and Architects
- Any other groups authorized to implement changes to the DGN or Crown Networks
- Disney Management Auditors
- Disney Global Information Security (GIS)

5 SCOPE

Location	Method Deployment
Theme Parks	Central Switched with L2 VPN
Guest Resorts	FlexConnect with ACL and Storm Control

6 ROAMING… A LAYER 2 STORY

Several factors go into the design of your roaming schema of a Wi-Fi wireless network. The concept of Wi-Fi is the extension of the LAN onto the Wireless. The definition of "extending" the network means that you are ether "Repeating" (layer 1) or "Bridging" (Layer 2) the information from one media to the other. When repeating; the action is one of limited buffering typically only 16 to 32 bits and then the pattern is "Repeated" onto the new medium. The use of repeating was first introduced into Ethernet networking in the 80's and has limited deployment uses as it also extends the "collision" domain.

In the case of modern Wi-Fi, we are bridging the Ethernet packets from the wireless side of the network to the LAN side. The wireless network receives the entire packet and then regenerates the packet onto the new medium with the appropriate headers, QoS, etc. In this manner the packets travel from wireless to wired in one direction and wired to wireless in the other. The Wi-Fi network is therefore a layer 2 medium for bridging traffic from a LAN based VLAN to a wireless based SSID. The controllers act as an aggregator and allow multiple APs to share the same VLAN/IP interface pair by performing the translation between the mediums and handling the support functions like radio management, key caching, etc. In some products such as HPE/Aurba, they elect to also provide layer 3 and above features such as routing, firewall, deep packet inspection, etc. These functions should be considered being applied after the bridging of the traffic from the wireless side of the network. To the client the wireless network is always a layer 2 story, and all other layers are transparent to the wireless supplicant.

6.1 SSID IS IT MORE THAN A NAME?

So what is an SSID and what role does it play in the ROAMING saga? The Service Set IDentifier ties the name like "WLAN-TWDC" to the Interface (VLAN/IP), Security, and other service specific parameters together. The concept in Wi-Fi is that a supplicant can migrate from AP to AP, as long as the supplicant attaches to the same SSID, the same "Services" will be available on the destination Access Point. Meaning the same VLAN/IP, the same security method, and special characteristics (11r, 11k, 11v, etc.) will be used to access the network. Most characteristics are considered optional and negotiated on a per association basis like the 11x features, the layer 3 network is expected to remain the same as Wi-Fi is a layer 2 technology.

What happens in our current configuration of the two distinct networks do not allow layer 2 roaming due to the utilization of different layer 3 interfaces (segmentation). Since the rest of the SSID is the same as far as security and name, the end device (supplicant) does not know it needs to request a new IP address and therefore fails to communicate on the network after a roam from Front to Back of House or vice versa. Where Front of House represents Crown and Back of House is the Atos supported networks.

6.2 PACKET ANALYSIS OF A ROAM

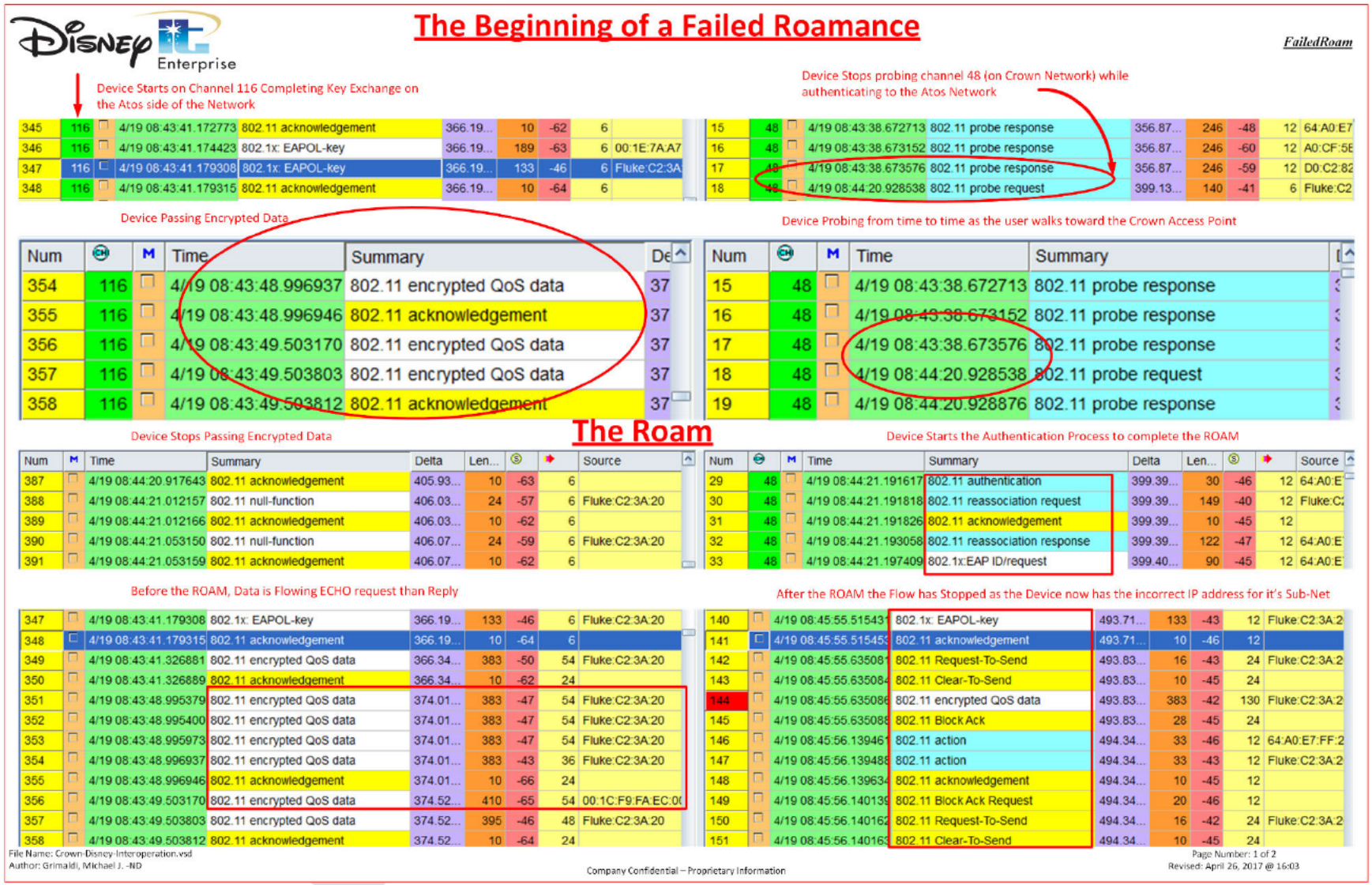
In the packet analysis we demonstrate the issue where in the case of the failed roam which was captured in our joint field trip. The failure was captured at Contemporary resort, while the successful roam was recorded at the Grand Floridian. The difference in the resorts is the Grand Floridian has been upgraded to the new configuration, where Contemporary has yet to be modified.

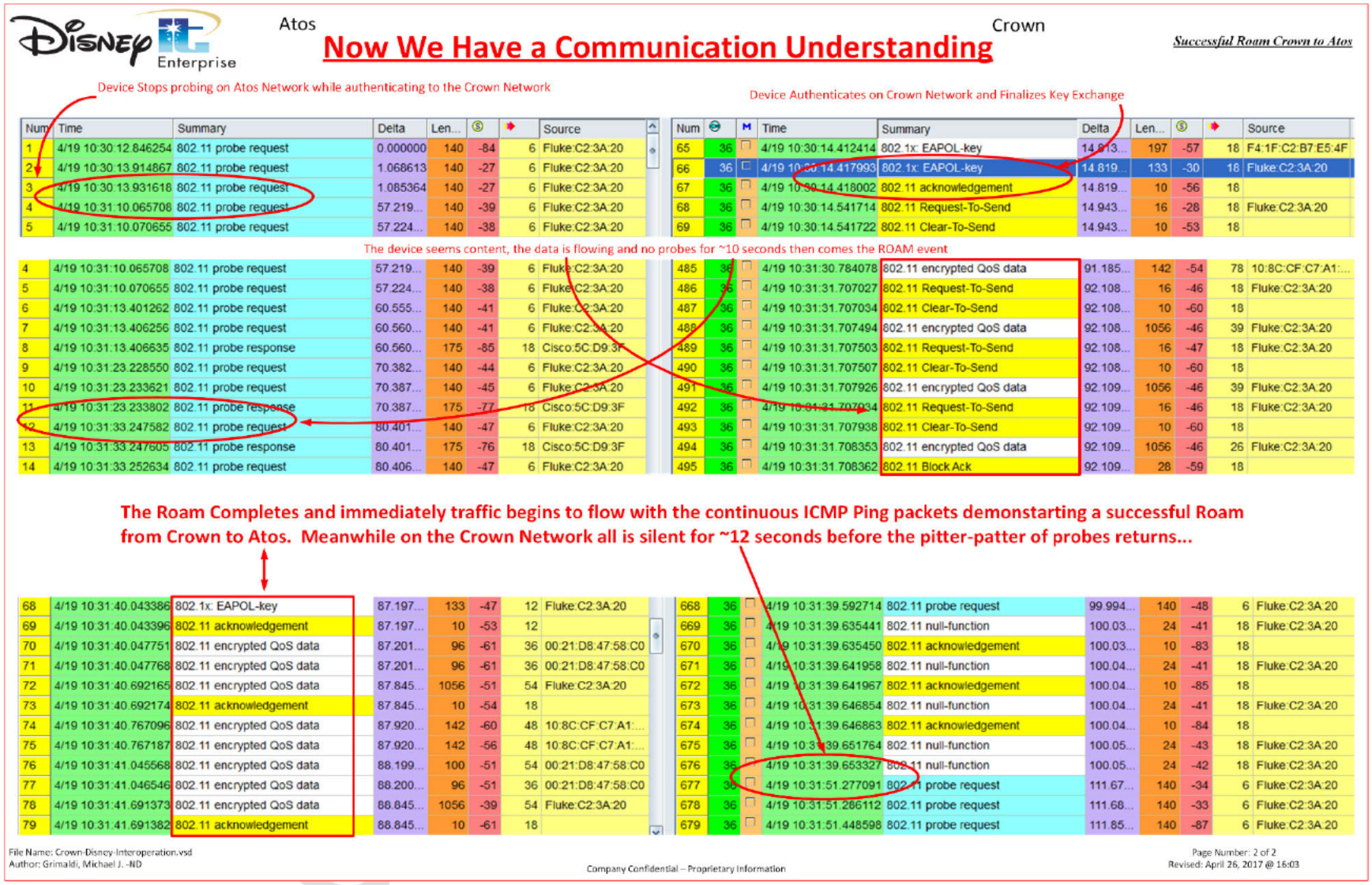
The test was conducted by initiating a Fluke One Touch to perform an endless test of ICMP Ping test against a server on the internet. The tester then walked from a Crown area or Access Point toward an Atos Access Point. The test was then repeated going from Atos to Crown. In every test the roam was predictable and consistently failed or succeeded based on the physical location of the test. The Grand Floridian allows layer 2 roaming between the network, whereas the Contemporary does not.

The conclusion of this testing shows that the ability to roam between networks is required and not an optional "nice to have". Just as we found that enabling roaming between our business partners that share the same building space, the same is true here and in the future. All Wi-Fi networks that are in close proximity of each other and advertise the same SSID, must provide roaming to be a "friendly" network of a cooperating partner.

When the manufactures of the Wi-Fi equipment are the same, such as both Cisco or both Aruba; then layer 3 roaming can be enabled by the use of controller to controller VPN. While this document does not cover the details of how this works, it is important to understand that in this configuration only transports user data is passed between the controllers. There is also session setup and teardown messages, but no control of device configuration or RF parameters are exchanged. This approach provides isolation between the networks in a similar fashion as a B2B VPN or Site2Site VPN, with the primary difference being the protocol and the initiation of the sessions. The layer 3 roam is named as it encapsulates the layer 2 information and transports it back to the devices assigned layer 3 interface. In this manner the end device can keep the same IP address as it roams from controller to controller.

The following section illustrates the layer 2 roam in a packet analysis. It shows both a failed roam from Contemporary Resort, and a successful roam recorded at the Grand Floridian Resort.


The Beginning of a Failed Roamance
FailedRoam
Disney IT Enterprise
Device Starts on Channel 116 Completing Key Exchange on the Atos side of the Network
Device Stops probing channel 48 (on Crown Network) while authenticating to the Atos Network
Device Passing Encrypted Data
Device Probing from time to time as the user walks toward the Crown Access Point
The Roam
Device Stops Passing Encrypted Data
Device Starts the Authentication Process to complete the ROAM
Before the ROAM, Data is Flowing ECHO request than Reply
After the ROAM the Flow has Stopped as the Device now has the incorrect IP address for it's Sub-Net
File Name: Crown-Disney-Interoperation.vsd
Author: Grimaldi, Michael J. -ND
Company Confidential – Proprietary Information
Page Number: 1 of 2
Revised: April 26, 2017 @ 16:03

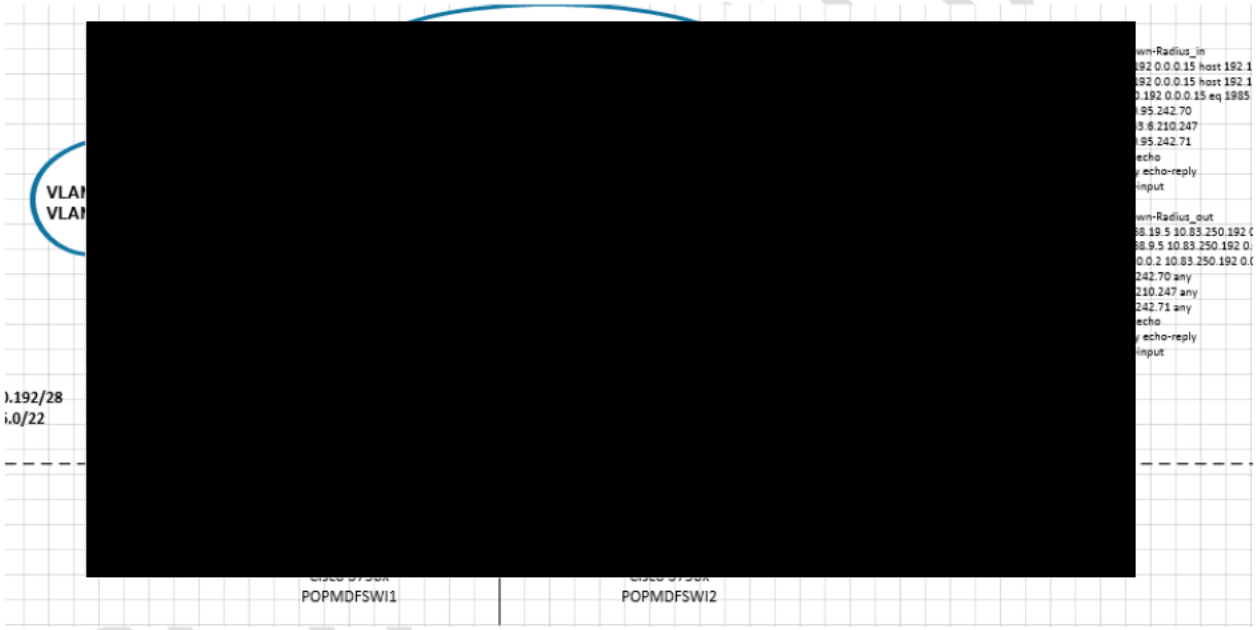

Disney IT Enterprise
Atos
Crown
Now We Have a Communication Understanding
Successful Roam Crown to Atos
Device Stops probing on Atos Network while authenticating to the Crown Network
Device Authenticates on Crown Network and Finalizes Key Exchange
The device seems content, the data is flowing and no probes for ~10 seconds then comes the ROAM event
The Roam Completes and immediately traffic begins to flow with the continuous ICMP Ping packets demonstarting a successful Roam from Crown to Atos. Meanwhile on the Crown Network all is silent for ~12 seconds before the pitter-patter of probes returns...
File Name: Crown-Disney-Interoperation.vsd
Author: Grimaldi, Michael J. -ND
Company Confidential – Proprietary Information
Page Number: 2 of 2
Revised: April 26, 2017 @ 16:03

7 GUEST RESORTS

[redacted]

7.1 PREVIOUS STATE:

[redacted]



[redacted]

7.2 WHAT IS CHANGING AND WHY:

Beyond the spanning-tree issues Disney and Crown operate independent networks which provides a boundary for users while roaming between the networks, and prevents a seamless transition from front to back-of-house. Because of the nature of wireless networks, the RF fields dose not honor the line between the networks and often bleeds into each other's space, causing additional roaming and stability issues for cast members.

To address this we modified the [redacted]

[redacted]

7.2.1 New Topology:

While this method works as the protocol was designed to work, there is a desirability to make the system consistent among all interconnected resorts. To provide consistency the recommendation is to allow [redacted] between the two Disney/Atos gateways.

In the revised plan notice that all secondary downstream switches for both Crown and Disney will be in blocking mode due to the additional path cost, and the revitalized path between the primary and secondary Disney/Atos gateways will now be the forwarding backup connection or designated root interface.

7.2.2 Risk Avoidance:

[redacted]

7.3 RESORT IMPLAMENTATION OF PCI SEGMENTATION

As discussed in part 2, the need to provide isolation of PCI enabled users from the general Disney User requires a modification to the method used to authenticate and transport the user traffic between Crown Castle and Atos managed networks. [redacted]

NOTE:

- **The default VLAN for all users will be [redacted] in the case of WDW Resort connectivity with Crown Castle.**
- **[redacted] is used for authentication traffic ONLY.**

8 PARKS INTERCONNECT MODIFICATIONS

[redacted]

[redacted]

The desire of this document and participating parties is to create a solution that is simple and supportable with the least amount of modification to our technology partner's network. To accomplish these goals we will be deploying a L2 VPN or "Pseudowire"

8.1 IMPLAMENTATION OF PCI SEGMENTATION

In addition to solving the roaming issue the need for a universal method of moving devices to the appropriate network was addressed in the previous sections. The need for profiles vs hardcoded VLAN numbers becomes clear when you consider the complexity of using multiple service providers and manufactures equipment. To facilitate the sustainability of a solution, [redacted] This approach will also allow each service provider the ability to upgrade and/or replace devices and manufactures without the need to redesign the overall architecture.

Location	Service Provider	Equipment Manufacture	Profile Name	Source IP Range	Notes
[redacted]					

Ex

Disney Enterprise

To provide multi-vendor/service provider roaming capability previously missing in the parks enviroment, the following MPLS AToM VPN technologies will be deployed.

WLAN-TWDC Interconnects
L2VPN-ParkServicesModel

Park	Pseudowire	PCI VLAN
Magic Kingdom	3030770	3730
Epcot	3030771	3731
Hollywood Studios	3030772	3732
Animal Kingdom	3030773	3733
ESPN	3030774	3734

Network Definitions
VLA[redacted]Auth 10.83.250.0/28
LON[redacted]on-PCI 10.83.X.0/20
LON[redacted]CI 10.114.X.0/21

[redacted] HSRP Host 10.83.250.14/28
0 HSRP Host 10.83.X.254/20
0 HSRP Host 10.114.X.254/2

Atos Managed

Crown Castel Managed

[redacted]

File Name: WLAN-TWDC Interconnects 07-06-2017 Master.v
Author: Grimaldi, Michael J.

[redacted]

The previous drawing shows the details of the new interconnection schema for Crown to Atos/DGN at the parks that support layer 3 interfacing. The concept utilizes the point-point L2VPN MPLS AToM technology to transport the back of house traffic from the DGN wireless controllers to the park gateways. The traffic will be combined with the front of house traffic on the indicated VLAN depending on if it is PCI or non-PCI traffic. Likewise the same VLAN will be extended down the trunks to the Crown Interconnection. This configuration will allow the same Layer 2 roaming domain be extended between the two service provider networks, without exposing ether management domains to the other.

[redacted] This will maintain park independence and isolation currently in place.

There is a lot going on for this drawing so let's break it down into the components. To begin with the way this type of layer 2 service is typically provided is a service provider edge (PE) to a customer provided edge (CE) equipment interchange. [redacted]. To emulate the functionality we will utiliz [redacted] This method will allow Crown to address and utilize the STP configuration most appropriate for their deployment. The DGN will not be exchanging STP information with Crown at the interface, just as the current solution is functioning today.

In the upper left of the drawing is a table that shows which [redacted]

The Blue lines represent the primary connection in solid and secondary dashed lines for secondary connections. [redacted]

[redacted]

[redacted]. This overarching architecture will be preserved in the new design. This design will add two additional VLANs temporary while configuration and deployment validation testing is underway. Once the transport is migrated to the new design, the old VLANs and routing interfaces will be removed from the configuration on both Crown and DGN networks.

Page is intentionally left blank