Multi-Platform Wireless Tool Assessment

A whitepaper by Abdurrahman Hassan

Contents

Introduction

As an engineer, we are constantly looking for tools that will help us troubleshoot various issues in a timely manner. When it comes to troubleshooting complex wireless situations the best use case is performing a packet capture, evaluating that data and arriving at a resolution. However, many times you are either troubleshooting from an AP perspective or you just don't have the means or resources to perform packet captures or gain site access to troubleshoot. Often-times we are at the mercy of the tools at our disposal and, depending on your place of employment, you will either have many tools to troubleshoot with or none at all.

Many wireless vendors have full-featured Web User Interfaces (WebUi) and we're going to break a few down in terms of application visibility and how we can use the tools at our disposal to remotely troubleshoot a wireless problem. In this whitepaper, I'm going to discuss certain features within your vendor AP infrastructure such as, Application Visibility and Control, SDWAN Network integration with wireless and DNA Center.

Application Visibility and Control

As technology grows so does our need of consuming data and reviewing information as quickly as we can. Companies are choosing to forgo the expensive costs of running cables and opting for more wireless devices in the workplace and, while this is welcomed, it may result in many updates taking place daily along with large file transfers. Client health and application visibility matter when troubleshooting application performance issues or complaints of overall performance at a branch site. The tools located within the wireless vendor solution help us, in our troubleshooting quest, to find the resolution as quickly as we possibly can.

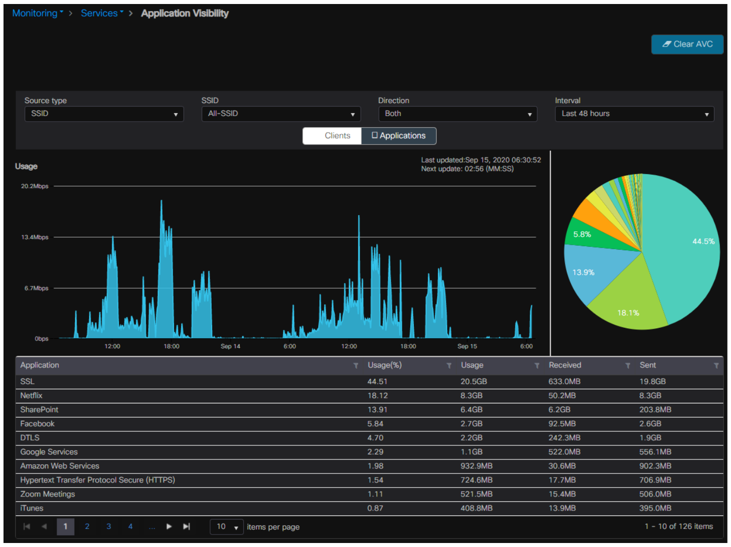
The Application Visibility and Control (AVC) solution is a suite of services in network devices that provide application-level classification, monitoring and traffic-control to improve business-critical application performance, facilitate capacity management and planning and reduce network operating costs.

This is not a definitive guide, but we'll touch upon some of the capabilities within each of these vendors. Please review each vendor website for a more in-depth look as to how they collect and produce AVC data.

- CISCO – www.cisco.com
- Aruba Networks – www.arubanetworks.com
- Extreme Networks – www.extremenetworks.com

CISCO

Figure 1 displays the AVC on a Cisco Embedded Wireless Controller or Wireless Lan Controller (WLC). Within this page you can review the type of application, usage percent, usage amount, and received and sent data. As an Example: AVC would help when trying to understand why a branch is suddenly experiencing bandwidth issues. As more and more devices are starting to come online wirelessly, views such as this help immensely when trying to get to the root cause of a problem. In this case, the engineer can point out high streaming traffic during business hours and work with internal teams to mitigate future impact. Additional filters can also be modified to view by SSID, direction, and interval for more granular data.



Source type: SSID
SSID: All-SSID
Direction: Both
Interval: Last 48 hours

Last updated:Sep 15, 2020 06:30:52
Next update: 02:56 (MM:SS)

Application	Usage(%)	Usage	Received	Sent
SSL	44.51	20.5GB	633.0MB	19.8GB
Netflix	18.12	8.3GB	50.2MB	8.3GB
SharePoint	13.91	6.4GB	6.2GB	203.8MB
Facebook	5.84	2.7GB	92.5MB	2.6GB
DTLS	4.70	2.2GB	242.3MB	1.9GB
Google Services	2.29	1.1GB	522.0MB	556.1MB
Amazon Web Services	1.98	932.9MB	30.6MB	902.3MB
Hypertext Transfer Protocol Secure (HTTPS)	1.54	724.6MB	17.7MB	706.9MB
Zoom Meetings	1.11	521.5MB	15.4MB	506.0MB
iTunes	0.87	408.8MB	13.9MB	395.0MB

10 items per page
1 - 10 of 126 items

Figure 1 – Cisco EWC AVC

Cisco bases its AVC around Deep Packet Inspection (DPI) that classifies more than 1400 applications. DPI can be thought of like checking your mail or Email (*Figure 2*). When you browse through your mail, you will refrain from opening any junk advertisements or simply throw them away. However, what you perceive as important mail will be opened and the contents within will be inspected. This is DPI in a nutshell. DPI evaluates the data part and the header of a packet that is transmitted through an inspection point and is able to locate, detect, categorize, block, or reroute packets that have specific code or data payloads that are not detected by conventional packet filtering.

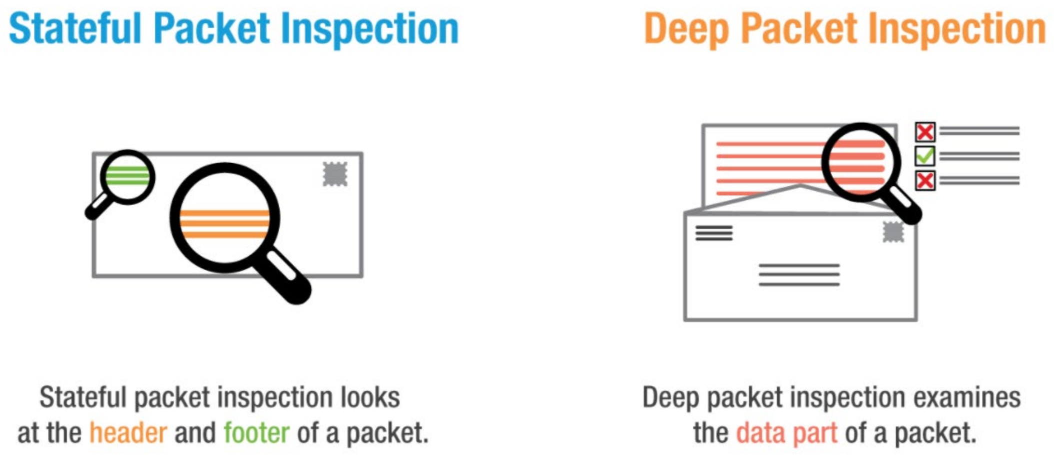

Stateful Packet Inspection
Deep Packet Inspection
Stateful packet inspection looks at the header and footer of a packet.
Deep packet inspection examines the data part of a packet.

Figure 2 – DPI Explanation

The following link highlights AVC and details how to configure it on a WLC as well as some caveats and restrictions to keep in mind when configuring it. AVC can be configured to either rate-limit, mark, or police traffic in either direction or reduce network congestion.

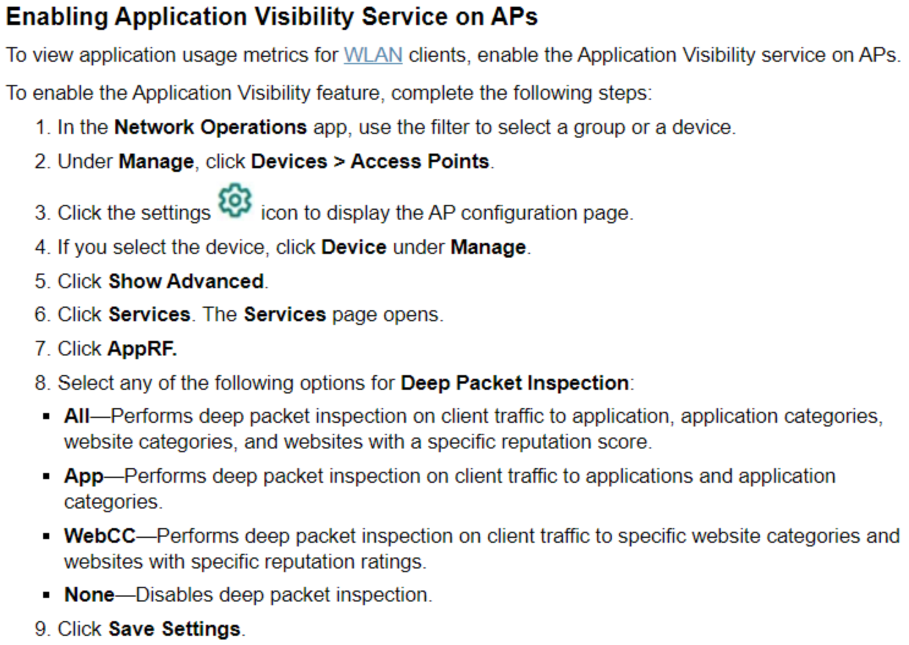
https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_01111.html

Aruba Networks

Controllers are still very much intact within the Aruba solution but as we head into 2021 and beyond Aruba Edge Services Platform (ESP) is taking shape with plans to deploy an AI-powered, cloud-native platform that enables you to unify, automate, and protect the edge. The result is moving controller services to the cloud and delivering maximum flexibility at enterprise scale.

Aruba Central with Instant AP's (IAP) integrates AVC and DPI with their custom-built, layer 7 firewall capability called AppRF. DPI, integrated with IAPs, opens the possibility to standardize traffic based on bandwidth control, QoS, and traffic shaping policies based around the most-used applications within the network. For example, that pesky personal streaming traffic can be blocked within the enterprise to free up bandwidth for more important applications.

Visibility on Aruba Central is disabled by default and can be enabled by following the directions in Figure 3.



Enabling Application Visibility Service on APs

To view application usage metrics for WLAN clients, enable the Application Visibility service on APs.

To enable the Application Visibility feature, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the settings ⚙ icon to display the AP configuration page.
4. If you select the device, click **Device** under **Manage**.
5. Click **Show Advanced**.
6. Click **Services**. The **Services** page opens.
7. Click **AppRF.**
8. Select any of the following options for **Deep Packet Inspection**:
   - **All**—Performs deep packet inspection on client traffic to application, application categories, website categories, and websites with a specific reputation score.
   - **App**—Performs deep packet inspection on client traffic to applications and application categories.
   - **WebCC**—Performs deep packet inspection on client traffic to specific website categories and websites with specific reputation ratings.
   - **None**—Disables deep packet inspection.
9. Click **Save Settings**.

Figure 3 – Enabling visibility (AppRF) on Aruba Central (source: ArubaNetworks.com)

Once AppRF is enabled you can start viewing the data on the Applications link on the left pane. Reviewing Figure 4, this page is broken down to four sections: Applications, Websites, Category and Blocked Traffic.

Applications – Includes a table view and graph view related to the client traffic flow to and from various applications

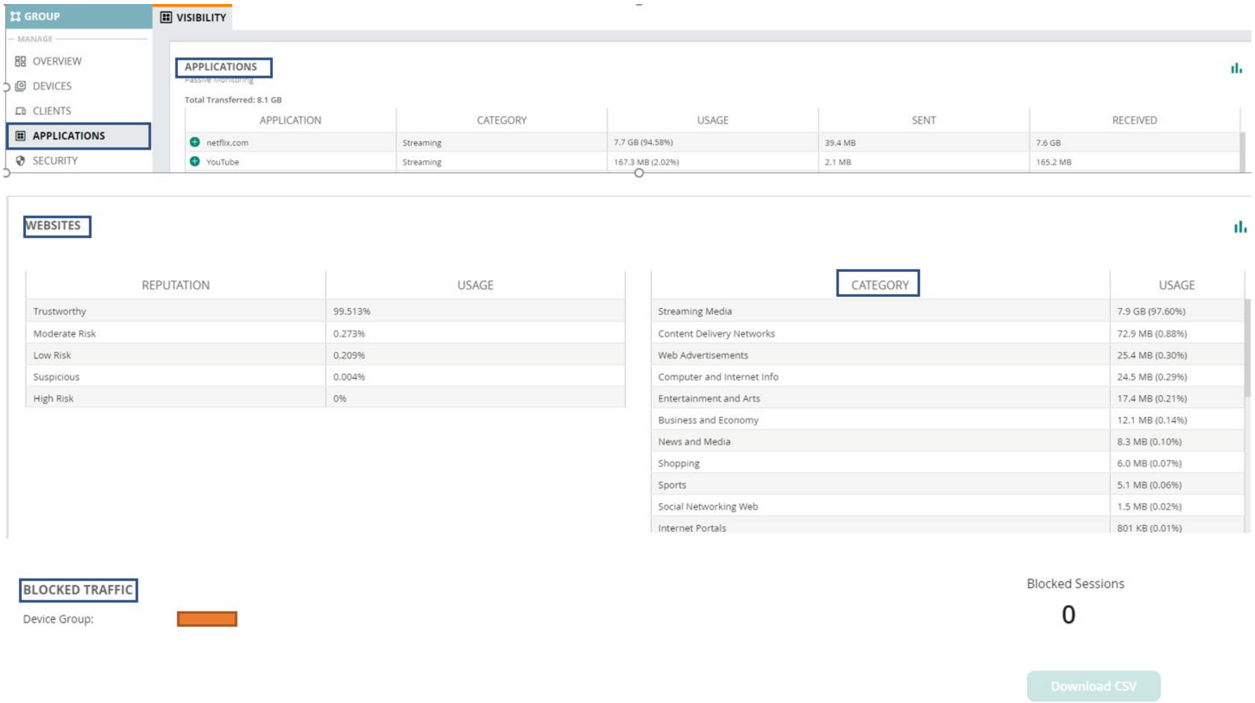
Websites – Includes as table view and bar graph view related to the client traffic flow to and from various websites

Category – Takes the data from the application section and categorizes traffic for a simpler view.

Blocked Traffic – Only shown for the IAP's on which Application Visibility or DPI ACL's are enabled.

For further knowledge on Aruba Central and how to set up AppRF with Visibility, please visit the following link:

https://help.central.arubanetworks.com/latest/documentation/online_help/content/access-points/mrt/app-visibility.htm



APPLICATIONS

Passive Monitoring

Total Transferred: 8.1 GB

APPLICATION	CATEGORY	USAGE	SENT	RECEIVED
netflix.com	Streaming	7.7 GB (94.58%)	39.4 MB	7.6 GB
YouTube	Streaming	167.3 MB (2.02%)	2.1 MB	165.2 MB

WEBSITES

REPUTATION	USAGE
Trustworthy	99.513%
Moderate Risk	0.273%
Low Risk	0.209%
Suspicious	0.004%
High Risk	0%

CATEGORY	USAGE
Streaming Media	7.9 GB (97.60%)
Content Delivery Networks	72.9 MB (0.88%)
Web Advertisements	25.4 MB (0.30%)
Computer and Internet Info	24.5 MB (0.29%)
Entertainment and Arts	17.4 MB (0.21%)
Business and Economy	12.1 MB (0.14%)
News and Media	8.3 MB (0.10%)
Shopping	6.0 MB (0.07%)
Sports	5.1 MB (0.06%)
Social Networking Web	1.5 MB (0.02%)
Internet Portals	801 KB (0.01%)

BLOCKED TRAFFIC

Device Group:

Blocked Sessions

0

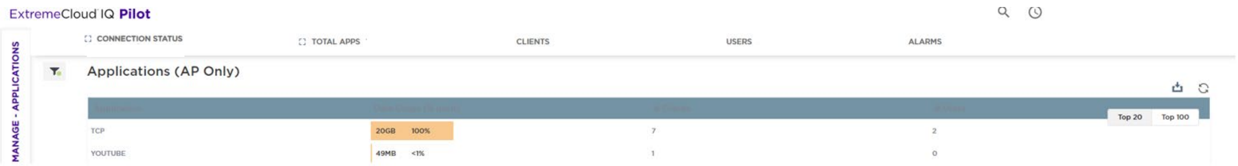
Figure 4 – Visibility view on Aruba Central

Extreme Networks

Compared to its competitors, Extreme Networks holds the assets of the early pioneer of cloud-based solutions through their acquisition of Aerohive Networks. Cloud-based architecture or "controller in the cloud" has become appealing to many businesses when it comes to expensive controller-based architecture with redundancy requirements. AP's within a controllerless architecture distribute all control functions and data forwarding to smart AP's while maintaining a centralized management system for monitoring and configuration.

ExtremeCloud IQ has over 1900 predefined application rules and counting. Custom applications and rules can also be built around your interesting traffic and assigned to your AP's. Applications can be assigned to various categories and detection rules can be set by type (Host Name, Server IP address & Port Number) and Protocol (HTTP & HTTPS).

Figure 5 details how applications traffic can be viewed either within the whole organization or per AP.



Applications (AP Only)

[illegible]	[illegible]	[illegible]	[illegible]
TCP	20GB 100%	7	2
YOUTUBE	49MB <1%	1	0

Figure 5 – Extreme Wireless Application Dashboard

Software Design Wide Area Networking

As an industry we are moving away from conventional network design and bringing the network in line with today's requirements. Businesses are looking for zero downtime and circuit redundancy while trying to save money in the overall bottom line. Regardless of how your network is setup, every business is seeking redundancy and resiliency that will help reduce downtime. We've talked about AVC within the wireless structure but we're going to step back and review the routing infrastructure with today's Software-Defined Wide Area Networking (SDWAN) offerings and how such a solution can help the user troubleshoot wireless in an effective manner.

Software-Defined Wide Area Networking (SDWAN) is a virtual WAN architecture that allow enterprises to leverage any combination of transport services – including MPLS, LTE and local internet services – to securely connect users to applications. With SDWAN the goal is to optimize traffic path for business-critical traffic, maximize uptime during circuit outages, and provide a single pane of glass when troubleshooting application and network issues. SDWAN solutions also provide the ability to fingerprint customer business applications and setup a local internet egress that would allow direct access to cloud resources.

As a wireless engineer we must tow the line and be aware of how wireless clients connect and pass traffic. This cannot be done without a well-placed network to complement the wireless infrastructure. We'll look at SilverPeak, which is one of the SDWAN companies ranked high in Gartner's Magic Quadrant (Figure 6).

SilverPeak & Wireless

SilverPeak includes sophisticated path conditioning techniques that can reconstruct packets lost in transit, avoiding retransmission. Essentially, Silver-Peak's Packet Order Correction overcomes performance issues of the underlying transport rather than simply routing traffic around the problem. This ultimately provides better resource utilization, higher application performance, improved productivity, a better user experience, and lower bandwidth costs.

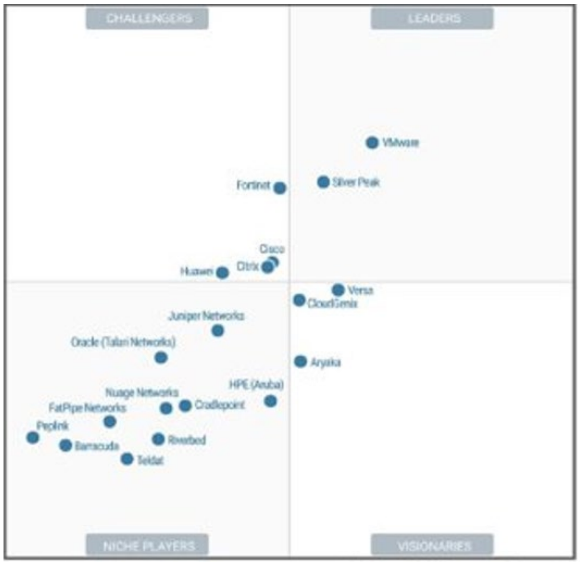
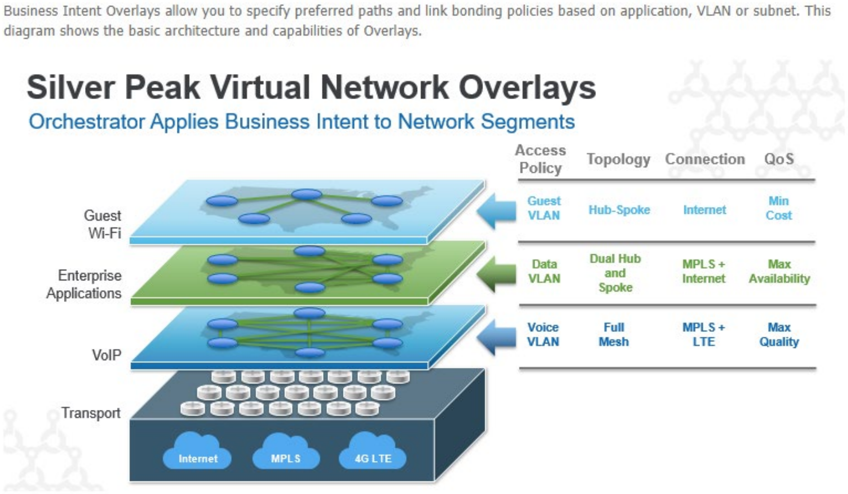


Figure 6 – Gartner Magic Quadrant

As displayed in Figure 7, application traffic is set within the Business Intent Overlay (BIO) profiles where traffic can be assigned policies and these policies are tied to certain thresholds that meet a routing criterion. While configuring a BIO (Figure 8) you can also set traffic to boost, which will enable WAN optimization, assign traffic to various firewall zones, assign traffic classes (Real-Time Traffic, Critical Apps, Bulk Apps), and implement QoS. *Please review additional documentation at Silver-Peak.com.*



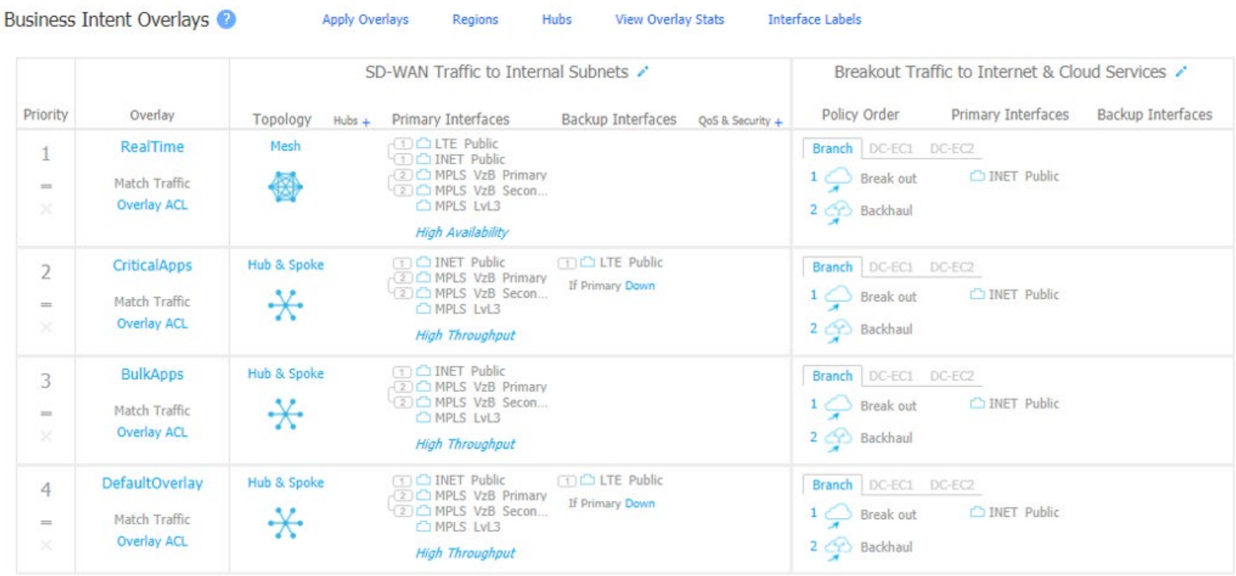
Business Intent Overlays allow you to specify preferred paths and link bonding policies based on application, VLAN or subnet. This diagram shows the basic architecture and capabilities of Overlays.

Silver Peak Virtual Network Overlays

Orchestrator Applies Business Intent to Network Segments

Access Policy	Topology	Connection	QoS
Guest VLAN	Hub-Spoke	Internet	Min Cost
Data VLAN	Dual Hub and Spoke	MPLS + Internet	Max Availability
Voice VLAN	Full Mesh	MPLS + LTE	Max Quality

Figure 7 – SilverPeak Virtual Network Overlays



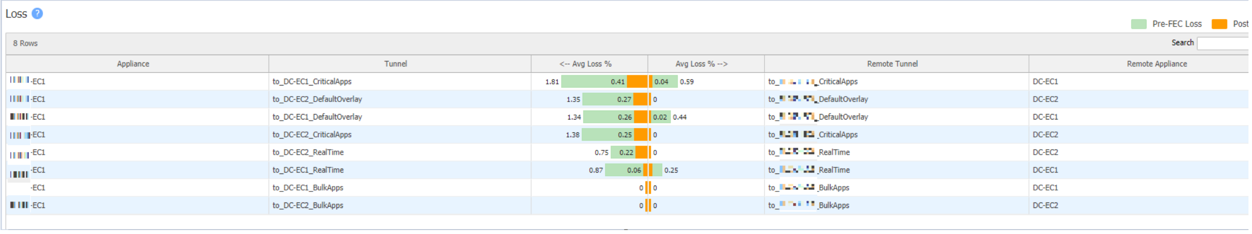
Business Intent Overlays ? Apply Overlays Regions Hubs View Overlay Stats Interface Labels

		SD-WAN Traffic to Internal Subnets				Breakout Traffic to Internet & Cloud Services		
Priority	Overlay	Topology Hubs +	Primary Interfaces	Backup Interfaces	QoS & Security +	Policy Order	Primary Interfaces	Backup Interfaces
1	RealTime Match Traffic Overlay ACL	Mesh	1 LTE Public 1 INET Public 2 MPLS VzB Primary 2 MPLS VzB Secon... MPLS LvL3 *High Availability*			Branch DC-EC1 DC-EC2 1 Break out 2 Backhaul	INET Public	
2	CriticalApps Match Traffic Overlay ACL	Hub & Spoke	1 INET Public 2 MPLS VzB Primary 2 MPLS VzB Secon... MPLS LvL3 *High Throughput*	1 LTE Public If Primary Down		Branch DC-EC1 DC-EC2 1 Break out 2 Backhaul	INET Public	
3	BulkApps Match Traffic Overlay ACL	Hub & Spoke	1 INET Public 2 MPLS VzB Primary 2 MPLS VzB Secon... MPLS LvL3 *High Throughput*			Branch DC-EC1 DC-EC2 1 Break out 2 Backhaul	INET Public	
4	DefaultOverlay Match Traffic Overlay ACL	Hub & Spoke	1 INET Public 2 MPLS VzB Primary 2 MPLS VzB Secon... MPLS LvL3 *High Throughput*	1 LTE Public If Primary Down		Branch DC-EC1 DC-EC2 1 Break out 2 Backhaul	INET Public	

Figure 8 – Business Intent Overlay Policies (BIO)

Setting these traffic policies are important when it comes to managing wireless traffic. Circuit failures or latency can affect applications on your client devices. Traffic for these clients can be prioritized within the SDWAN structure to ensure nothing else takes priority over it. SDWAN increasingly helps Voice over Wi-Fi (VoWi-Fi) with QoS and ensures packets are kept in order to provide a constant stream of communication. We talked about Packet Order Correction or Forward Error Correction (FEC) earlier and this is where it comes into play within the SDWAN structure. When dealing with VoWi-Fi you are looking for ideal roam times and prioritized QoS. This situation coupled with SDWAN ensures communication is ongoing as the VoWi-Fi devices are moving around.

Figure 9 highlights the pre & post Forward Error Correction (FEC) loss between the SilverPeak equipment at the branch and the Data Center. The results are packets being repaired prior to the end of the conversation which results in unbroken communication.



Loss ?

🟩 Pre-FEC Loss 🟧 Post

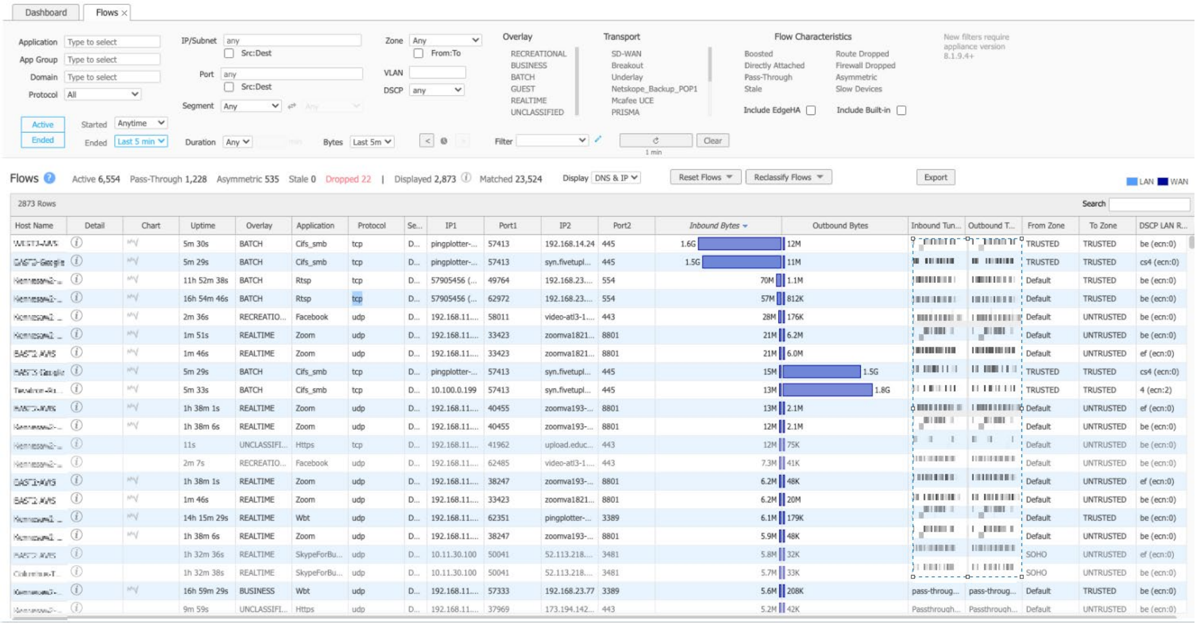
8 Rows

Search

Appliance	Tunnel	<-- Avg Loss %	Avg Loss % -->	Remote Tunnel	Remote Appliance
[redacted]-EC1	to_DC-EC1_CriticalApps	1.81 0.41	0.04 0.59	to_[redacted]_CriticalApps	DC-EC1
[redacted]-EC1	to_DC-EC2_DefaultOverlay	1.35 0.27	0	to_[redacted]_DefaultOverlay	DC-EC2
[redacted]-EC1	to_DC-EC1_DefaultOverlay	1.34 0.26	0.02 0.44	to_[redacted]_DefaultOverlay	DC-EC1
[redacted]-EC1	to_DC-EC2_CriticalApps	1.38 0.25	0	to_[redacted]_CriticalApps	DC-EC2
[redacted]-EC1	to_DC-EC2_RealTime	0.75 0.22	0	to_[redacted]_RealTime	DC-EC2
[redacted]-EC1	to_DC-EC1_RealTime	0.87 0.06	0.25	to_[redacted]_RealTime	DC-EC1
[redacted]-EC1	to_DC-EC1_BulkApps	0	0	to_[redacted]_BulkApps	DC-EC1
[redacted]-EC1	to_DC-EC2_BulkApps	0	0	to_[redacted]_BulkApps	DC-EC2

Figure 9 – FEC Loss

Figure 10 displays flow of traffic in real-time as it traverses the network. This is an additional tool that can be used to find wireless client data and discover what type of applications it is trying to communication with. Figure 11 shows a more granular view of a flow and provides a wealth of information to sift through, specifically QoS and type of traffic and more.



Application: Type to select
App Group: Type to select
Domain: Type to select
Protocol: All
IP/Subnet: any ☐ Src:Dest
Port: any ☐ Src:Dest
Segment: Any
Zone: Any ☐ From:To
VLAN:
DSCP: any

Overlay: RECREATIONAL, BUSINESS, BATCH, GUEST, REALTIME, UNCLASSIFIED
Transport: SD-WAN, Breakout, Underlay, Netskope_Backup_POP1, Mcafee UCE, PRISMA
Flow Characteristics: Boosted, Directly Attached, Pass-Through, Stale, Route Dropped, Firewall Dropped, Asymmetric, Slow Devices
Include EdgeHA ☐ Include Built-in ☐
New filters require appliance version 8.1.9.4+

Active / Ended — Started: Anytime — Ended: Last 5 min — Duration: Any — Bytes: Last 5m — Filter:

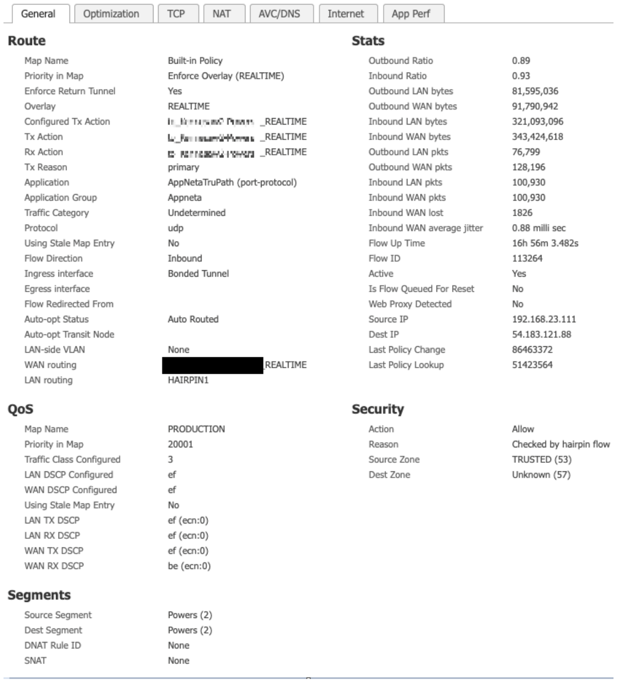
Flows — Active 6,554 Pass-Through 1,228 Asymmetric 535 Stale 0 Dropped 22 | Displayed 2,873 Matched 23,524 — Display: DNS & IP

2873 Rows

Host Name	Detail	Chart	Uptime	Overlay	Application	Protocol	Se...	IP1	Port1	IP2	Port2	Inbound Bytes	Outbound Bytes	Inbound Tun...	Outbound T...	From Zone	To Zone	DSCP LAN R...
[redacted]	ⓘ	〰	5m 30s	BATCH	Cifs_smb	tcp	D...	pingplotter-...	57413	192.168.14.24	445	1.6G	12M	[redacted]	[redacted]	TRUSTED	TRUSTED	be (ecn:0)
[redacted]	ⓘ	〰	5m 29s	BATCH	Cifs_smb	tcp	D...	pingplotter-...	57413	syn.fivetupl...	445	1.5G	11M	[redacted]	[redacted]	TRUSTED	TRUSTED	cs4 (ecn:0)
[redacted]	ⓘ	〰	11h 52m 38s	BATCH	Rtsp	tcp	D...	57905456 (...	49764	192.168.23....	554	70M	1.1M	[redacted]	[redacted]	Default	TRUSTED	be (ecn:0)
[redacted]	ⓘ	〰	16h 54m 46s	BATCH	Rtsp	tcp	D...	57905456 (...	62972	192.168.23....	554	57M	812K	[redacted]	[redacted]	Default	TRUSTED	be (ecn:0)
[redacted]	ⓘ	〰	2m 36s	RECREATIO...	Facebook	udp	D...	192.168.11....	58011	video-atl3-1....	443	28M	176K	[redacted]	[redacted]	Default	UNTRUSTED	be (ecn:0)
[redacted]	ⓘ	〰	1m 51s	REALTIME	Zoom	udp	D...	192.168.11....	33423	zoomva1821...	8801	21M	6.2M	[redacted]	[redacted]	Default	UNTRUSTED	be (ecn:0)
[redacted]	ⓘ	〰	1m 46s	REALTIME	Zoom	udp	D...	192.168.11....	33423	zoomva1821...	8801	21M	6.0M	[redacted]	[redacted]	Default	UNTRUSTED	ef (ecn:0)
[redacted]	ⓘ	〰	5m 29s	BATCH	Cifs_smb	tcp	D...	pingplotter-...	57413	syn.fivetupl...	445	15M	1.5G	[redacted]	[redacted]	TRUSTED	TRUSTED	cs4 (ecn:0)
[redacted]	ⓘ	〰	5m 33s	BATCH	Cifs_smb	tcp	D...	10.100.0.199	57413	syn.fivetupl...	445	13M	1.8G	[redacted]	[redacted]	TRUSTED	TRUSTED	4 (ecn:2)
[redacted]	ⓘ	〰	1h 38m 1s	REALTIME	Zoom	udp	D...	192.168.11....	40455	zoomva193-...	8801	13M	2.1M	[redacted]	[redacted]	Default	UNTRUSTED	ef (ecn:0)
[redacted]	ⓘ	〰	1h 38m 6s	REALTIME	Zoom	udp	D...	192.168.11....	40455	zoomva193-...	8801	12M	2.1M	[redacted]	[redacted]	Default	UNTRUSTED	be (ecn:0)
[redacted]	ⓘ		11s	UNCLASSIFI...	Https	tcp	D...	192.168.11....	41962	upload.educ...	443	12M	75K	[redacted]	[redacted]	Default	UNTRUSTED	be (ecn:0)
[redacted]	ⓘ		2m 7s	RECREATIO...	Facebook	udp	D...	192.168.11....	62485	video-atl3-1....	443	7.3M	41K	[redacted]	[redacted]	Default	UNTRUSTED	be (ecn:0)
[redacted]	ⓘ	〰	1h 38m 1s	REALTIME	Zoom	udp	D...	192.168.11....	38247	zoomva193-...	8801	6.2M	48K	[redacted]	[redacted]	Default	UNTRUSTED	ef (ecn:0)
[redacted]	ⓘ	〰	1m 46s	REALTIME	Zoom	udp	D...	192.168.11....	33423	zoomva1821...	8801	6.2M	20M	[redacted]	[redacted]	Default	UNTRUSTED	be (ecn:0)
[redacted]	ⓘ	〰	14h 15m 29s	REALTIME	Wbt	udp	D...	192.168.11....	62351	pingplotter-...	3389	6.1M	179K	[redacted]	[redacted]	Default	TRUSTED	be (ecn:0)
[redacted]	ⓘ	〰	1h 38m 6s	REALTIME	Zoom	udp	D...	192.168.11....	38247	zoomva193-...	8801	5.9M	48K	[redacted]	[redacted]	Default	UNTRUSTED	be (ecn:0)
[redacted]	ⓘ		1h 32m 36s	REALTIME	SkypeForBu...	udp	D...	10.11.30.100	50041	52.113.218....	3481	5.8M	32K	[redacted]	[redacted]	SOHO	UNTRUSTED	ef (ecn:0)
[redacted]	ⓘ		1h 32m 38s	REALTIME	SkypeForBu...	udp	D...	10.11.30.100	50041	52.113.218....	3481	5.7M	33K	[redacted]	[redacted]	SOHO	UNTRUSTED	be (ecn:0)
[redacted]	ⓘ	〰	16h 59m 29s	BUSINESS	Wbt	udp	D...	192.168.11....	57333	192.168.23.77	3389	5.6M	208K	pass-throug...	pass-throug...	Default	TRUSTED	be (ecn:0)
[redacted]	ⓘ		9m 59s	UNCLASSIFI...	Https	udp	D...	192.168.11....	37969	173.194.142...	443	5.2M	42K	Passthrough...	Passthrough...	Default	UNTRUSTED	be (ecn:0)

Figure 10 – Silver Peak Flows

I've only touched on a few items related to what SDWAN has to offer. Like various wireless AP vendors, there are many SDWAN companies out there with their own secret sauce mixed into their solution that makes them unique. However, the overall outcome is the same: redundancy, resiliency, and minimal to no downtime. I would urge anyone reading this to review the many SDWAN flavors and reach out to a local partner if you require further information.



Route

Map Name	Built-in Policy
Priority in Map	Enforce Overlay (REALTIME)
Enforce Return Tunnel	Yes
Overlay	REALTIME
Configured Tx Action	[redacted]_REALTIME
Tx Action	[redacted]_REALTIME
Rx Action	[redacted]_REALTIME
Tx Reason	primary
Application	AppNetaTruPath (port-protocol)
Application Group	Appneta
Traffic Category	Undetermined
Protocol	udp
Using Stale Map Entry	No
Flow Direction	Inbound
Ingress interface	Bonded Tunnel
Egress interface	
Flow Redirected From	
Auto-opt Status	Auto Routed
Auto-opt Transit Node	
LAN-side VLAN	None
WAN routing	[redacted]_REALTIME
LAN routing	HAIRPIN1

Stats

Outbound Ratio	0.89
Inbound Ratio	0.93
Outbound LAN bytes	81,595,036
Outbound WAN bytes	91,790,942
Inbound LAN bytes	321,093,096
Inbound WAN bytes	343,424,618
Outbound LAN pkts	76,799
Outbound WAN pkts	128,196
Inbound LAN pkts	100,930
Inbound WAN pkts	100,930
Inbound WAN lost	1826
Inbound WAN average jitter	0.88 milli sec
Flow Up Time	16h 56m 3.482s
Flow ID	113264
Active	Yes
Is Flow Queued For Reset	No
Web Proxy Detected	No
Source IP	192.168.23.111
Dest IP	54.183.121.88
Last Policy Change	86463372
Last Policy Lookup	51423564

QoS

Map Name	PRODUCTION
Priority in Map	20001
Traffic Class Configured	3
LAN DSCP Configured	ef
WAN DSCP Configured	ef
Using Stale Map Entry	No
LAN TX DSCP	ef (ecn:0)
LAN RX DSCP	ef (ecn:0)
WAN TX DSCP	ef (ecn:0)
WAN RX DSCP	be (ecn:0)

Security

Action	Allow
Reason	Checked by hairpin flow
Source Zone	TRUSTED (53)
Dest Zone	Unknown (57)

Segments

Source Segment	Powers (2)
Dest Segment	Powers (2)
DNAT Rule ID	None
SNAT	None

Figure 11 – SilverPeak Flow Detail

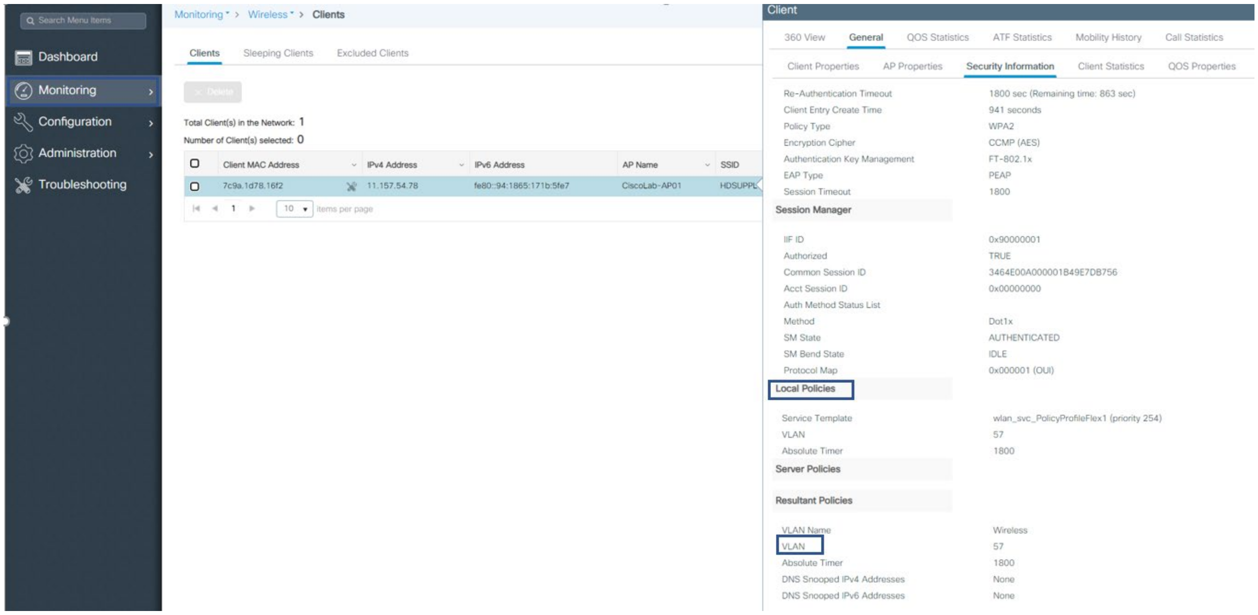
Additional Client Troubleshooting Tools

In the next few sections, we'll look at some additional ways to troubleshoot client related issues from a Cisco and Extreme Wireless perspective. Let's look into the following management systems and review the various ways to ingest the data and work your way to a quicker resolution.

- Cisco Client 360 View
- WLC Configuration
- Extreme Client View
- DNA Center – Wireless Assurance

Cisco Client 360 View

Client related issues can easily be reviewed via the left pane: Monitoring > Clients. As seen on Figure 12, navigating to this area will display a client 360 view of how the client is connected to a specific SSID, local policies the client is assigned to and which VLAN is set on the policy. These are just a few of the items listed and there are many sub-levels you can click through to obtain more granular data. A client complaining of connectivity issues can be reviewed here and, for example, you may determine that an incorrect policy was applied which placed the client in to an incorrect VLAN.



Total Client(s) in the Network: 1
Number of Client(s) selected: 0

□	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID
□	7c9a.1d78.16f2	11.157.54.78	fe80::94:1865:171b:5fe7	CiscoLab-AP01	HDSUPPL

1 · 10 items per page

Re-Authentication Timeout	1800 sec (Remaining time: 863 sec)
Client Entry Create Time	941 seconds
Policy Type	WPA2
Encryption Cipher	CCMP (AES)
Authentication Key Management	FT-802.1x
EAP Type	PEAP
Session Timeout	1800
Session Manager	
IIF ID	0x90000001
Authorized	TRUE
Common Session ID	3464E00A000001B49E7DB756
Acct Session ID	0x00000000
Auth Method Status List	
Method	Dot1x
SM State	AUTHENTICATED
SM Bend State	IDLE
Protocol Map	0x000001 (OUI)
Local Policies	
Service Template	wlan_svc_PolicyProfileFlex1 (priority 254)
VLAN	57
Absolute Timer	1800
Server Policies	
Resultant Policies	
VLAN Name	Wireless
VLAN	57
Absolute Timer	1800
DNS Snooped IPv4 Addresses	None
DNS Snooped IPv6 Addresses	None

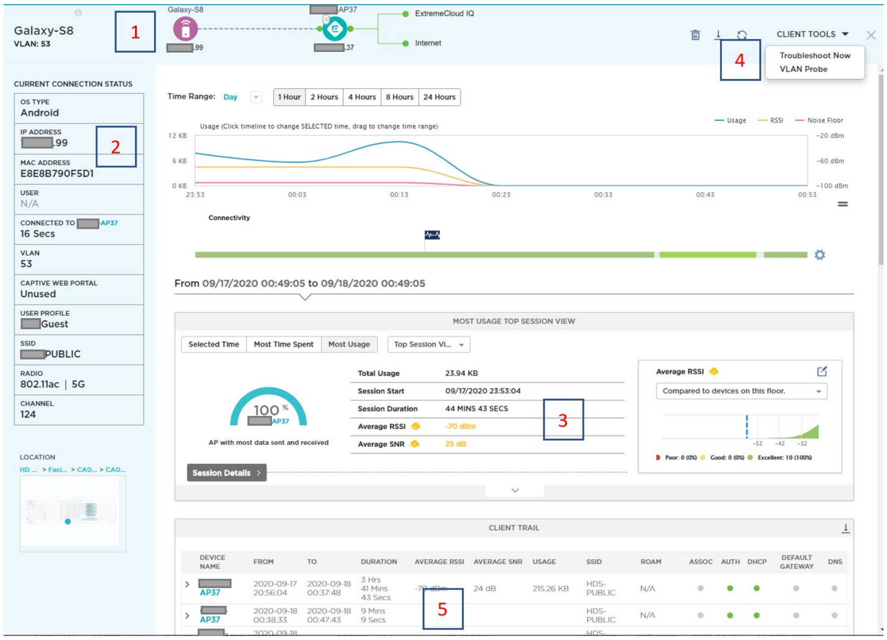
Figure 12 – Client Monitoring

WLC Configuration

As you've spent time with the new 9800 WLC platform from CISCO you'll begin to wonder if some type of cheat code has been entered to obtain the deep level of configuration options within the platform. It is important to be aware and to have a firm understanding of what each level of configuration accomplishes prior to updating configurations. Most Radio profile changes will cause temporary loss of client connectivity so be cautious when making updates during business hours. A worthy mention would be the ability to obtain packet captures over the air with little effort and a packet capture can be generated for a client and then viewed with Wireshark or another protocol analyzer.

Extreme Client View

Extreme client view offers a world of information when it comes to client troubleshooting. Let's look at Figure 13 and unpack the various levels of data to understand how this page alone can be used to troubleshoot various client issues.



Galaxy-S8
VLAN: 53

CURRENT CONNECTION STATUS

OS TYPE
Android

IP ADDRESS
[redacted].99

MAC ADDRESS
E8E8B790F5D1

USER
N/A

CONNECTED TO [redacted]AP37
16 Secs

VLAN
53

CAPTIVE WEB PORTAL
Unused

USER PROFILE
[redacted]Guest

SSID
[redacted]PUBLIC

RADIO
802.11ac | 5G

CHANNEL
124

From 09/17/2020 00:49:05 to 09/18/2020 00:49:05

MOST USAGE TOP SESSION VIEW

Total Usage	23.94 KB
Session Start	09/17/2020 23:53:04
Session Duration	44 MINS 43 SECS
Average RSSI	-70 dBm
Average SNR	25 dB

Average RSSI

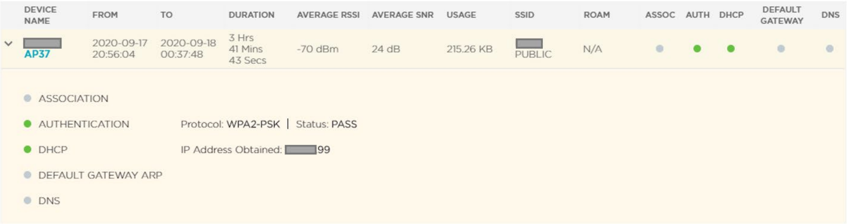
Poor: 0 (0%) Good: 0 (0%) Excellent: 10 (100%)

CLIENT TRAIL

	DEVICE NAME	FROM	TO	DURATION	AVERAGE RSSI	AVERAGE SNR	USAGE	SSID	ROAM	ASSOC	AUTH	DHCP	DEFAULT GATEWAY	DNS
>	[redacted] AP37	2020-09-17 20:56:04	2020-09-18 00:37:48	3 Hrs 41 Mins 43 Secs	-70 dBm	24 dB	215.26 KB	HDS-PUBLIC	N/A	●	●	●	●	●
>	[redacted] AP37	2020-09-18 00:38:33	2020-09-18 00:47:43	9 Mins 9 Secs				HDS-PUBLIC	N/A	●	●	●	●	●
	[redacted]	2020-09-18						HDS-						

Figure 13 – Client View

1. Graphical view of how the client is connected to the network.
2. MAC address, IP address, VLAN, Profile, SSID and Channel information is displayed on the left pane.
3. AP information is listed here and at what RSSI and SNR the client is connected to the Ap compared to other devices in the vicinity
4. Client tools
   a. Troubleshoot now will take you to another page where you can collect packet captures from an AP and review client data
   b. VLAN Probe – By far the most popular troubleshooting tool within the platform. This tool can be used to check which VLAN's are allowed and in this case if VLAN 53 produces no result then you know there is a misconfiguration. Reviewing switch ports would then show VLAN 53 was not allowed on the trunk port and allowing the port will successfully authenticate the client.
5. Client Trail
   a. As a client device roams between AP's a client trail will be gathered of the interaction with the device and AP's. Figure 14 expands a client trail view where authentication and DHCP were successful. Unsuccessful results will yield a red dot and advise the engineer where to begin troubleshooting.



	DEVICE NAME	FROM	TO	DURATION	AVERAGE RSSI	AVERAGE SNR	USAGE	SSID	ROAM	ASSOC	AUTH	DHCP	DEFAULT GATEWAY	DNS
⌄	[redacted] AP37	2020-09-17 20:56:04	2020-09-18 00:37:48	3 Hrs 41 Mins 43 Secs	-70 dBm	24 dB	215.26 KB	[redacted] PUBLIC	N/A	●	●	●	●	●

● ASSOCIATION

● AUTHENTICATION   Protocol: WPA2-PSK | Status: PASS

● DHCP   IP Address Obtained: [redacted]99

● DEFAULT GATEWAY ARP

● DNS

Figure 14 – Client Trail

DNA CENTER – Wireless Assurance

DNA Center is another tool within the Cisco ecosystem that offers the opportunity to view wireless data at a more granular level. WLCs and APs can be onboarded into DNA center where data can be collected and populated via the DNA Center Assurance view. There's a lot to unpack here, so we'll dig into some of the important views and details. I'd urge anyone reading this to review DNA Center documentation on Cisco.com or reach out to their vendor partner for additional information.

Wireless Assurance, within the DNA Center (DNAC), takes your data beyond the WLC and populates AP, client health, and application data under one single pane of glass. It should be said that DNAC only complements Cisco-based devices when it comes to assurance. Figure 15 displays the overall health of wired and wireless clients. As you can see from the image, I'm having an issue on one of the APs, so let's dig in to see what is going on.

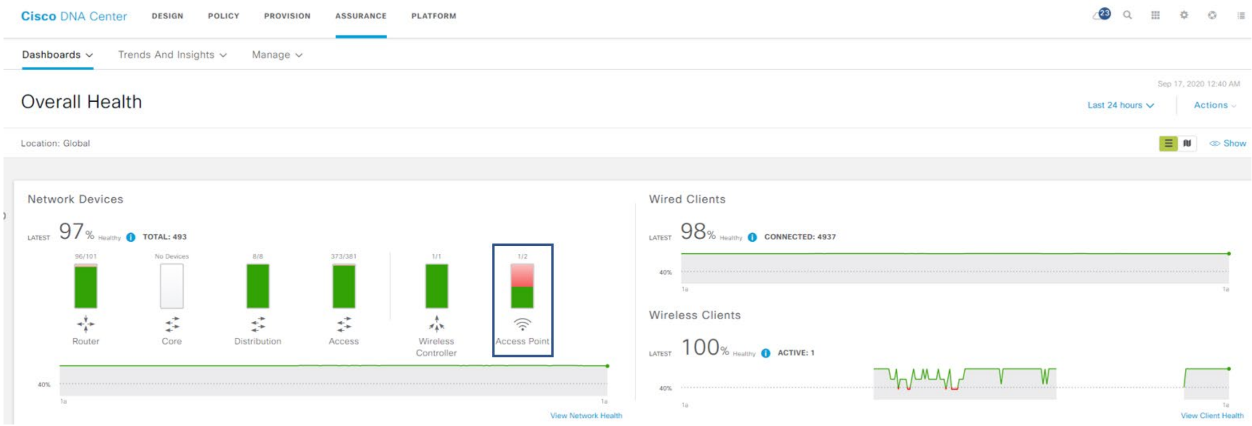
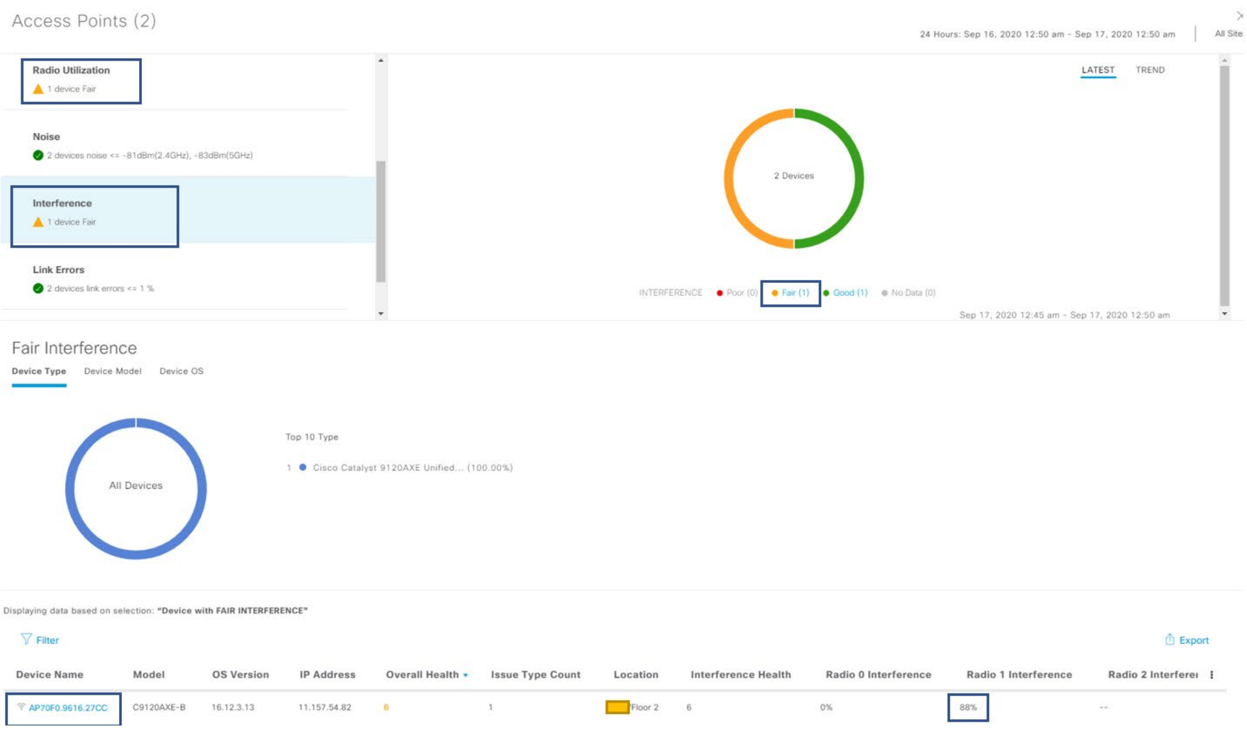


Figure 15 – Overall Health

As I click through the network health I'm brought to the area where I can see that there is an issue with one AP. A summary on the left pane provides me with an explanation as to what the issue is (Figure 16). As you can see, it is Fair Radio Utilization and some type of interference is occurring. I'm also given the AP name, location, and Radio interference percentage.



Access Points (2)

24 Hours: Sep 16, 2020 12:50 am - Sep 17, 2020 12:50 am | All Site

Radio Utilization
▲ 1 device Fair

Noise
✓ 2 devices noise <= -81dBm(2.4GHz), -83dBm(5GHz)

Interference
▲ 1 device Fair

Link Errors
✓ 2 devices link errors <= 1 %

Sep 17, 2020 12:45 am - Sep 17, 2020 12:50 am

Fair Interference

Top 10 Type

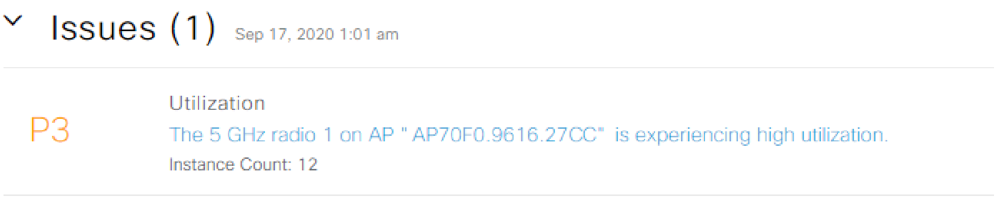
1 ● Cisco Catalyst 9120AXE Unified... (100.00%)

Displaying data based on selection: **"Device with FAIR INTERFERENCE"**

Device Name	Model	OS Version	IP Address	Overall Health	Issue Type Count	Location	Interference Health	Radio 0 Interference	Radio 1 Interference	Radio 2 Interferei
AP70F0.9616.27CC	C9120AXE-B	16.12.3.13	11.157.54.82	6	1	Floor 2	6	0%	88%	--

Figure 16 – Radio Utilization

I can then click on the AP name, which takes me to Device 360, where it provides me with information about the AP. The Issues section in Figure 17 alerts me to the fact that my 5GHz radio on this AP is experiencing high utilization. As I click on the issue seen in Figure 18, I'm given a list of troubleshooting steps to perform to come to a resolution.



Issues (1) Sep 17, 2020 1:01 am

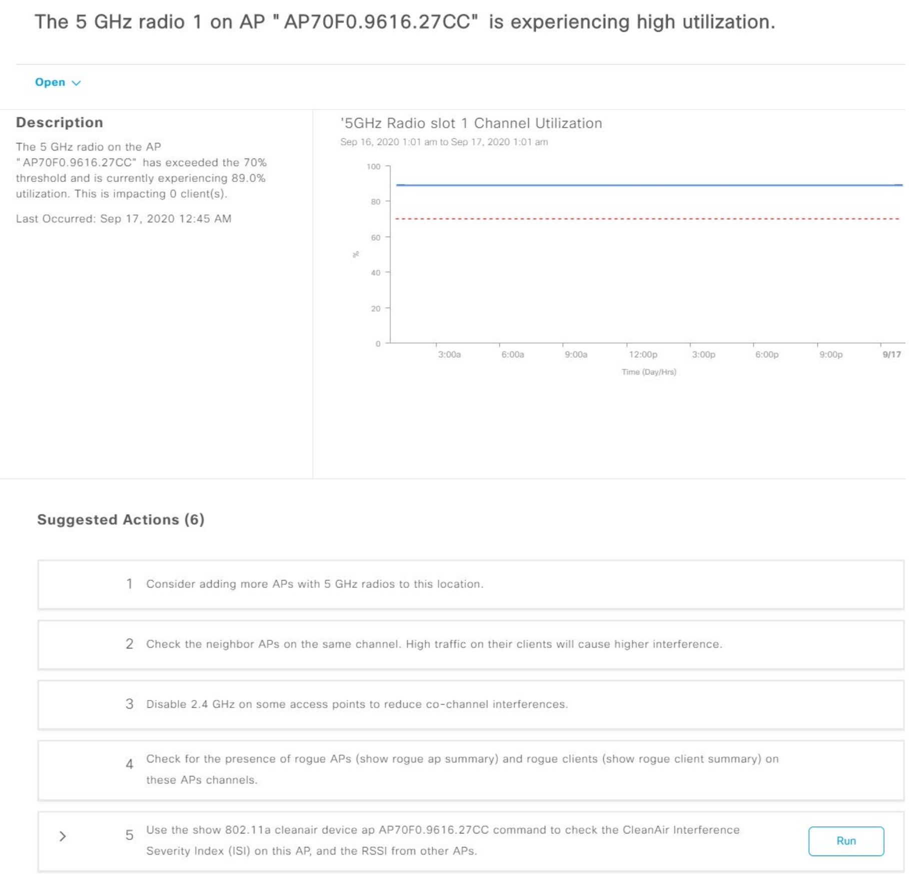
P3

Utilization

The 5 GHz radio 1 on AP " AP70F0.9616.27CC" is experiencing high utilization.

Instance Count: 12

Figure 17 – Issues view



The 5 GHz radio 1 on AP " AP70F0.9616.27CC" is experiencing high utilization.

Description

The 5 GHz radio on the AP " AP70F0.9616.27CC" has exceeded the 70% threshold and is currently experiencing 89.0% utilization. This is impacting 0 client(s).

Last Occurred: Sep 17, 2020 12:45 AM

'5GHz Radio slot 1 Channel Utilization

Sep 16, 2020 1:01 am to Sep 17, 2020 1:01 am

Suggested Actions (6)

1 Consider adding more APs with 5 GHz radios to this location.

2 Check the neighbor APs on the same channel. High traffic on their clients will cause higher interference.

3 Disable 2.4 GHz on some access points to reduce co-channel interferences.

4 Check for the presence of rogue APs (show rogue ap summary) and rogue clients (show rogue client summary) on these APs channels.

5 Use the show 802.11a cleanair device ap AP70F0.9616.27CC command to check the CleanAir Interference Severity Index (ISI) on this AP, and the RSSI from other APs.

Figure 18 – AP Troubleshooting View

Within the Device 360 view, you'll also have the following views:

Physical Topology View – Network map showing devices connected

Event Viewer – List of ongoing events over a period of time

Path Trace – Run tests to find location of the issue

Detail Information – Information for the AP detailing Device, Connectivity and RF accompanied with graphical views

DNAC also offers a Client 360 view which is like Device 360 but from a client perspective. From this view you can review authentication times, application experience, detailed client information and how they are connected to the wireless (VLAN, Band, Channel Width and so on).

DNA Center, if implemented correctly, can be used as another medium to troubleshoot AP, client, and application health issues. Once configured, DNA Center can also pull intelligent packet captures or collect information from Cisco based sensors and have that data populated as another means of troubleshooting.

SUMMARY

Troubleshooting wireless in any environment is a challenge and, as an engineer, we're always looking for the quickest road to resolution. There are many tools at our disposal that allow us the functionality to perform various tests and determine root causes. As detailed above, each wireless vendor is unique in tools they provide to assist with troubleshooting. As the engineer troubleshooting a specific situation, we must possess the knowledge of how to use these tools and, at the same time, appease any frustration displayed by the client.

References:

https://devopedia.org/deep-packet-inspection

www.arubanetworks.com

www.cisco.com

www.silver-peak.com