DNA Analytics and Assurance– The Shortest Path to Network Innocence!

Tony Hsieh thsieh@cisco.com

The "Why" of Cisco



Ciscolive!

IT Priorities Survey—2017

Does your organization currently have a digital transformation initiative underway?



ZK Research 2017 IT Priorities Survey

Ciscolive,

https://blogs.cisco.com/enterprise/why-digital-success-depends-on-the-right-network https://engage2demand.cisco.com/LP=8802

Why Transform Digitally?

 According to Harvard Business Review, companies that master digital transformation generate:

more revenue than their industry peers, and

26% more profits than their industry peers



TURNING TECHNOLOGY INTO BUSINESS TRANSFORMATION

GEORGE WESTERMAN I DIDIER BONNET I ANDREW MCAFEE

https://hbr.org/product/leading-digital-turning-technology-into-business-transformation/17039E-KND-ENG

ciscolive!



Transforming Customer Experiences



BURBERRY

Transforming Customer Experiences

0

HERI

Transforming Employee Experiences





BHHE 3X more organizations intend to be digital ready in

> 2 YEARS - IDC¹

ciscolive!

Business at the Speed of Digital

"Digital business requires faster delivery of services to the business, ultimately requiring enterprises to change network operations processes and tooling."

– Gartner²

. IDC Digital Network Readiness Survey – Commissioned Survey by Cisco

Gartner: Predicts 2017: Enterprise Networks and Network Services Published: 18 November 2016 ID: G0031642

Achieving Business Agility via Network Architecture

Ciscolive!

 "Digital success depends on being able to move with speed and capturing opportunities faster than the competition. This requires a dynamic and flexible IT foundation. However, a business is only as agile as its least agile component and, in many cases today, that's the network."



—a ZK Research, Digital Success White-Paper, 2017.

10

Unprecedented Demands on the Network



The Need for a New Network



Constantly Learning

Support 100X new devices, apps, users





Constantly Adapting

Respond Instantly to business demands with limited staff and budget



Constantly Protecting

See and predict issues and threats and respond fast

The more you use it, the smarter it gets.



THE NETWORK. INTUITIVE. Powered by intent, informed by context.





"It takes [us] 4 months and \$1M to push a QoS change...

I view the administrator as being a business analyst via a central station without needing to have any understanding of QoS models and low level device attributes"

-Wall Street Financial Customer

Ciscolive

Legacy QoS Policy

ip access-list extended APIC_EM-MM_STREAM-ACL remark citrix - Citrix permit tcp anv anv eg 1494 permit udp any any eq 1494 permit tcp any any eq 2598 permit udp anv anv eg 2598 remark citrix-static - Citrix-Static permit tcp any any eq 1604 permit udp any any eq 1604 permit tcp any any range 2512 2513 permit udp any any range 2512 2513 remark pcoip - PCoIP permit tcp any any eq 4172 permit udp any any eq 4172 permit tcp any any eq 5172 permit udp any any eq 5172 remark timbuktu - Timbuktu permit tcp any any eq 407 permit udp any any eq 407 remark xwindows - XWindows permit tcp any any range 6000 6003 remark vnc - VNC permit tcp any any eq 5800 permit udp any any eq 5800 permit tcp any any range 5900 5901 permit udp any any range 5900 5901 exit ip access-list extended APIC EM-SIGNALING-ACL remark h323 - H.323 permit tcp any any eq 1300 permit udp any any eq 1300 permit tcp any any range 1718 1720

Intent-Based **Application Policy**



Apply Policy

MY CRITICAL APP

Deploy End-to-End QoS Policies in Minutes



Ciscolive,

BRKSDN-2777 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public 16

"QoS rollouts were once 6-month projects costing over \$200K. With Cisco APIC EM Easy QoS, we will go from months to minutes with nominal costs."

BRIAN MCEVOY

Symantec Sr Network Engineer

Cisco Live Berlin Keynote Video (~21 min in)

https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=93610&backBtn=true

Software Defined Access Secure Segmentation and Onboarding



IT Simplicity

- No VLAN, ACLs or IP Address management required
- Single network fabric
- Define one consistent policy

Security

- Simplified Micro-Segmentation
- Policy enforcement

Completely Automated | Policy follows Identity | Minimize Lateral Threat Movement ciscolive: © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public 18

SD-Access Business Value Delivered





BOV Improvement in Issue Resolution



https://www.ciscolive.com/latam/learn/keynotes/

Ciscolive,

19 BRKSDN-2777 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

THE NETWORK. INTUITIVE. Powered by intent, informed by context.

LEARNING CONTEXT INTENT SECURITY

Where is IT Spending Their Time?

Finding the Source of an issue, is a complex, end-to-end problem



Ciscolive!

Transforming the Network with Big Data Analytics



The Value of Context

"By all means go and see this play"

—Theatre Critic

(as quoted in an advertisement by the play's performers)

ciscolive!

BRKSDN-2777 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public 23

The Value of Context

"If triviality is what you happen to be wanting, by all means go and see this play"

—Theatre Critic

Ciscolive!



Ciscolive!



Ciscolive!



Ciscolive,



Ciscolive,



BRKSDN-2777 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public 29

Ciscolive,

Ciscolive!



BRKSDN-2777 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public 30



THE NETWORK. INTUITIVE. Powered by intent, informed by context.

LEARNING INTENT CONTEXT SECURITY

What is Machine Learning?

- Machine learning is an application of **artificial intelligence** (AI) that provides systems the ability to automatically learn and improve from experience without being explicitly programmed to do so
- The process of learning begins with observations of data, and **looking for patterns** within the data so as to make **increasingly better** correlations, inferences and predictions
- The primary aim is to allow these systems to learn automatically without human intervention or assistance and adjust actions accordingly



Ciscolive



Ciscolive!

THE NETWORK. INTUITIVE. Powered by intent, informed by context.



The Network MUST be secure!

Target Data Breach Spilled Info On As Many As 70 Million Customers

🛛 🕧 💟 🛅 😣



Maggie McGrath, FORBES STAFF Food, retail, and consumerism in an age of voting with dollars FULL BIO ✓

The data breach that was the nightmare before Christmas for Target TOT +#35% and its millions of customers just got a little bit worse: the retailer said Friday morning that the information stolen between November 27 and December 15, 2013 included personal information of as many as 70 million people -- more than the 40 million the company originally estimated.

On December 19, the retailer said that as many as 40 million credit card and debit card accounts may have been compromised during Black Friday weekend through December 15, and that information stolen included customer names, credit or debit card number, the card's expiration date and CVV (card verification value). Now, in an update on the hacking investigation, Target said that an additional 70 million people were affected, and the stolen customer information includes names, mailing address that much of this data is "partial in nature," but it will nonetheless provide one protection to all guests who shopped at its U.S. stores.

The Equifax breach may have exposed 143 million people's Social Security numbers — but here's why you shouldn't freak out



The Equifax data breach was

serious.

Equifax, one of the three credit reporting agencies in the US, announced that it was compromised between mid-May and July, potentially exposing Social Security numbers, credit card numbers, and other personal information for up to 143 million Americans.

The company hasn't handled it well so far. People are pissed, and they have a right to be. On top of

BRKSDN-2777



EMAIL

Online security is flimsier than we like to admit. APJJosh Reynolds

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public 36


The Network MUST be secure!

🕬 Wana Decrypt0r 2.0		۲.
	Ooops, your files have been encrypted! English	-
	What Happened to My Computer? Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.	
Payment will be raised on	Can I Recover My Files?	-
5/15/2017 23:37:34	Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.	
Time Left	You can decrypt some of your files for free. Try now by clicking <decrypt>. But if you want to decrypt all your files, you need to pay.</decrypt>	
	You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.	
	We will have free events for users who are so poor that they couldn't pay in 6 months.	
5/19/2017 23:37:34	How Do I Pay?	
Time Left	Please check the current price of Bitcoin and buy some bitcoins. For more information,	
A6: 23: 38: 28	click <how bitcoins="" buy="" to="">. And send the correct amount to the address specified in this window.</how>	
	After your payment, click <check payment="">. Best time to check: 9:00am - 11:00am</check>	-
About hiteoin	Send \$300 worth of bitcoin to this address:	
How to buy bitcoins?	ACCEPTED HERE 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94	y
Contact Us	Check Payment Decrypt	
li al		

Ciscol(VC;

Encryption is changing the threat landscape



Enterprises are embracing encryption but so are attackers

80%

of organizations are victims of malicious activity

41%

Of attacks used encrypted traffic to evade detection

Problem Statement

How can we identify malware without decrypting traffic? Is this even solvable?



Providing Security While Maintaining Privacy!

Encrypted Traffic Analytics (ETA) Visibility and malware detection without decryption



Malware in encrypted traffic

Is the payload within the TLS session malicious?

- · End to end confidentiality
- Channel integrity during inspection
- · Adapts with encryption standards



Cryptographic compliance

How much of my digital business uses strong encryption?

- · Audit for TLS policy violations
- Passive detection of Ciphersuite vulnerabilities
- Continuous monitoring of network opacity

Ciscolive

How can we inspect encrypted traffic?



ciscolive!

Initial Data Packet (IDP) Analysis

- HTTPS header contains several information-rich fields.
- Server name provides domain information.
- Crypto information educates us on client and server behavior and application identity.
- Certificate information is similar to **whois** information for a domain.
- And much more can be understood when we combine the information with global data.





Benign vs. Malicious Behavior



Ciscolive!

BRKSDN-2777 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public 43

Sequence of Packet Lengths and Times Analysis: Google Search Example



Ciscolive,

BRKSDN-2777 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public 44

Sequence of Packet Lengths and Times Analysis: Bestafera Example





Malware detection using Cognitive Analytics



All three elements reinforce each other inside the analytics engine using them.

What is "Client Assurance"?

You may want to know how your clients are doing... in two cases:

- Troubleshooting
 - Support calls, can't connect, can't ping XYZ... what happened? Why?
- Design Improvement Lifecycle
 - How many clients can I get here? What is the breaking point for application X? What is traffic likely to look like in 6 months? What do I need to change, anticipate?



DNA Assurance Client Issue Page



Ciscolive!

What are "Issues" in Assurance

Assurance "issues" have at least two angles:

- Population process
 - How we define issues, define their detection, cause and remediation
- Display process
 - How we display in the UI information about issues, insights, trends



Population Process – Building Blocks

Ciscolive!

An "issue" is potentially composed of up to 4 elements



Sometimes, Symptom and Issue are the same ("can't associate to Wi-Fi") Sometimes Issue and Cause are the same

(e.g. Symptom = AP fails to join WLC; Issue/Cause = WLC reboots)

BRKSDN-2777 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public 50

Population Process – Where to Start From?

We can work on Issues starting from any of the first 3 blocks



Ciscolive!

The Symptom-based approach is tempting because this is what users report However, its risk is the wild goose chase ("what if it is because...")

Population Process – Where to Start From?

We can work on Issues starting from any of the first 3 blocks



Because Issue can be the symptom, this can be a slippery process



Population Process – Where to Start From?

Third Block is Safest to Work From



Causes can be Issues (or not), but they are always traceable events that may have impact on users or network



Population Process – Event Listing

Working from Causes can be done in many ways, we chose the *Follow The Path* approach





Population Process – Correlation Map

Once Causes are defined, we can map them to Issues and Symptoms

What Issue can this trigger:

- Reachability (GW, server)
- Service failures
- Performances (slow throughput)
- Etc.

What symptom will be associated: We need to define some of them, but not all of them, as per our Display logic (see later slides)

Link is flapping because of STP issue





Population Process – Grouping "Issues"

The Correlation Map is a mesh, with many to many relationships

- A single cause can be source of multiple issues
- A single issue can result in multiple symptoms
- A single issue can be cause by multiple different causes

Multiple possible symptoms		Multiple possible causes
A		Α
В	GW Reachability issue	B
С		0
D		
F		
_		E



Individual client check:



Ciscolive!

Continuous global checks:





Individual client check:

802.11 auth, worked, on time802.11 assoc, worked, on time



Ciscolive!

Individual client check:

All worked well until EAP request
Never got the EAP response



We know that the issue is "on the client side" How far can we dig?

- AP on WLC okay? (RTT, CAPWAP keepalives, etc.)
- Other clients on same WLAN okay?
- Client RSSI/SNR/retries?
- Is-it an EAP compatibility issue?



Surfacing the issue in the UI:

- We want to be process-efficient, all these checks are built in a Russian doll, and a mesh logic
- For example:
 - RF problems cause AAA and other issues
 - A broken AP affects many clients
 - A broken AAA affects all new clients
 - Etc.
- In other words: surface the larger issue first





Client on boarding and connectivity insights



Issues - client boarding issue



DNA Assurance Client Issue Page



BRKSDN-2777

Excessive IP Addressing

We know:

- 802.11 auth, assoc were okay, on time
- AAA phases worked, on time
- Client sent a DHCP request
- DHCP responded, but late (based on baseline)
- Why?
 - Network issue
 - Server issue
 - Service issue



Issues - client boarding issue



Life, Once You Have Onboarded

Roaming can be an issue

• "Roaming is the same as onboarding, except that we know the client already"

Client RF may suffer

- Sticky client
- Ping-pong client
- Poor RF client
- CHDM client

Quality of experience can degrade outside of RF issues



Issues - Wireless connected categories



Kairos

Ciscolive

Issues - Wireless connected categories



Kairos

Ciscolive

DNA Assurance Workflows

	Client experience	Network experience	Application experience
	(Access)	(Connectivity)	(Performance)
Single user	1. <u>Single-user onboarding</u> : association,	2. Single-user connectivity: connectivity	3. <u>Single-user application experience</u> :
	authentication, and addressing for	to network services and applications	application performance experience
	end-user devices	for end-user devices	for end-user devices
Multiple users	4. <u>Multi-user onboarding</u> : association,	5. <u>Multi-user connectivity</u> : connectivity	6. <u>Multi-user application experience</u> :
	authentication, and addressing for	to network devices and applications	application performance for multiple
	multiple end-user devices	for multiple end-user devices	end-user devices
Multi-site		7. <u>Site connectivity</u> : geographic / topology view of connectivity to network devices and applications	8. <u>Site application performance</u> : geographic / topology view of application performance

9. Compliance: network device configuration, QoS policies, ACLs, licenses, and software version

10. Management: reporting, thresholds, sensors

11. Single-user self-guided: end-user details for device information, connectivity, policies, and RF

12. Multi-user self-guided: network device details for device information, connectivity, policies, view configuration, connect-to-device and fabric

13. Telemetry: User click interaction with UI, dwell time per page, flows between pages, issue and health feedback, dynamic survey, and make a wish

Ciscolive!

ONA Assurance is More than Wi-Fi Clients



✓ Over 100+ Actionable Insights

Wireless	Switching	Routing
66	38	8



SDA and Switching Specific Correlated Insights

			Client Onboarding	
Control plane reachability Edge reachability Border reachability Routing protocol MAP server	Border and edge connectivity Border node health Access node health Network Services DHCP, DNS, AAA	ISE/PxGrid connectivity Border Node policy Edge Node policy	Client/Device DHCP Client/Device DNS Client authentication / authorization	CPU, Mem, Temp Line-card Modules POE power TCAM Table

Total SDA/Switching Insights: 38 issues in DNA-C 1.1



BRKSDN-2777 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public 72
Wireless Specific Correlated Insights

Client Onboarding	Client Experience	Network Coverage & Capacity	Network Device Monitoring	Application Performance Sensor
Association failures Authentication failures IP address failure Client Exclusion Excessive on-boarding time Excessive authentication time Excessive IP addressing time	Throughput analysis Roaming pattern analysis Sticky client Slow roaming Excessive roaming RF, Roaming pattern Dual band clients prefer 2.4GHz	Coverage hole AP License Utilization Client Capacity Radio Utilization	Availability Crash, AP Join Failure High Availability CPU, Memory utilization Flapping AP, Hung Radio Power supply failures	Web: HTTP & HTTPS Email: POP3, IMAP, Outlook Web Access File Transfer: FTP & TFTP Terminal: Telnet & SSHv2

Total Insights: 66 issues in DNA-C 1.1

Ciscolive!



Sun Oct 22 2017 21:33:01 GMT-0700 (Pacific Standard Time)

Sun Oct 22 2017 21:19:01 GMT-0700 (Pacific Standard Time)

Sun Oct 22 2017 21:11:01 GMT-0700 (Pacific Standard Time)

Los Angeles

Los Angeles

Los Angeles



ONA-C Assurance Apple Insights

Ciscolive!

LA1-AP3802-31

LA1-AP3802-31

LA1-AP3802-31

cl_ST_DEVICE_IDLE

cl_ST_DEVICE_IDLE

cl_ST_DEVICE_IDLE

Network Health



Network Health—Site View

	DESIGN POLICY	PROVISION AS	SURANCE					Q. 11	¢	=
Health 🗸 Dashboard	ls 🗸 Issues	Manage 🗸								
overall health	lealth						All Domains 🗸	Jan 22	, 2018 3:31	pm
©24 Hours ✓	3:25p 6:00p	 9:00р	1/22	 3:00a	 6:00a	 9:00a 1	3:25p Ⅰ Ⅰ Ⅰ 1 2:00p 3:00p	<>		
Location: Global/USA								≡ * (Hide
+ Daks				Bu	ırbank	Fiintnoge	Altadena			
Agoura Hills	Calabasas	adapt a	17			Glendale	Pasadena	Monrovia Arcadia Duar	le /	Azusa '
		Topanga State Park		West Hollywo	od	ENX ?	Alhambra	a to	win Park	Covi
				Beverly Hills		Los Angeles	Roseme Monterey-Park	EL Monte ead South El Monte	West Cov	ina 😽
State	valiou	Santa	Monica				Montebello			Feedba
			P			Huntington Park	S HEALTHY	• <40% • 40~79% •	Jos roal	D 76teiç

Network Health—Topology View



Network Health—By Device Roles



78

Network Health—Device 360 (Part 1 of 3)



Ciscolive

Network Health—Device 360 (Part 2 of 3)

CISCO CENTER	DESIGN	POLICY	PROVISION	ASSURANCE	Q	 ٥	:=

✓ Physical Neighbor Topology Last Updated: 01/22/18 03:42:50 pm ○ Refresh

EQ Find by device IP, device type, MAC ...





Network Health—Device 360 (Part 3 of 3)



Network Issues and Troubleshooting Example—Part 1 of 4



Network Issues and Troubleshooting Example—Part 2 of 4

ealth ~ Dashboard 71% Healthy Devices	Wireless clients failed to conner Status: Open ~	ect (Site: Glo	bal/USA/Lo	s Angel	es/Level	16) – DH	CP Timed	DUT 8 2:30 F
View Network H	Description Clients located in " Global/USA/Los Angeles/Level 16" timed out and have not been assigned an IP address from the DHCP	Impacted Wirele	ess Clients Im	≣Q , Find				
Top 10 Issues (8)	server.	Hostname 👻	Mac Address	Device Type	AP	SSID / VLAN	WLC	I
Connectivity OSPF Adjacency Failed	 Location: 1 Building Clients 	Mirna-PC	B8:27:EB:0C:57:C8	WIRELESS	LA1- AP3802-11	LA-Guest1 / 130	LA1- WLC5520-1	
Total occurrences: 822		Leigh-PC	B8:27:EB:0C:53:E0	WIRELESS	LA1- AP3802-11	LA-Guest1 / 130	LA1- WLC5520-1	
Connectivity OSPF Adjacency Failed Total occurrences: 850	5 Wireless Clients	Ethelyn-PC	B8:27:EB:0C:48:28	WIRELESS	LA1- AP3802-11	LA-Guest1 / 130	LA1- WLC5520-1	
Onboarding Wireless clients failed t Total occurrences: 48			Authenticatio	n <	•			
Onboarding Wireless clients failed t	Suggested Actions (8)							

Total occurrences: 48

Network Issues and Troubleshooting Example—Part 3 of 4

CISCO CENTER DE	ESIGN POLICY PROVISION ASSURANCE	ii 0	1
Health V Dashboard	Wireless clients failed to connect (Site: Global/USA/Los Angeles/Level 16) - DHCP - Status: Open ~	Time	> out 8 2:30 PM
	Suggested Actions (8)		
Top 10 Issues (8)	1 Verify that the DHCP scope is configured correctly and has adequate free IP addresses since the DHCP server will not respond if the DHCP scope is used up.		
Connectivity OSPF Adjacency Failed Total occurrences: 822	2 Reduce the DHCP lease time so that clients that are gone do not continue to be assigned an IP address. Best practice - DHCP lease time for high-density, high mobile environment is 15-30 min.		
Connectivity OSPF Adjacency Failed Total occurrences: 850	3 Verify that the IP helper address on the router is configured correctly to make sure the DHCP server is gettign the DHCP messages from the client.		
Onboarding Wireless clients failed t Total occurrences: 48	4 Verify that the DHCP server has a route to the VLAN's subnet.		
Onboarding Wireless clients failed t Total occurrences: 48	5 Check whether the clients moved during the IP addressing phase.	84	

Network Issues and Troubleshooting Example—Part 4 of 4

CISCO CENTER DE	SIGN POLICY PROVISION ASSURANCE	Q Ⅲ Φ Ⅲ
Health V Dashboard	OSPF Adjacency Failed on Device "10.30.255.2" Interface GigabitEthe Neighbor 10.30.255.101	ernet0/0/1 with
View Network H	Status: Open V	Last Occurred: Jan 21, 2018 2:49 PM
	Suggested Actions (6)	
_	\sim Ø 1 Ping the neighbor IP to verify connectivity.	
Top 10 Issues (8)	🧭 ping neighbor IP	
Connectivity OSPF Adjacency Failed Total occurrences: 822	ping 10.30.255.101 ping 10.30.255.101 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.30.255.101, timeout is 2 seconds:	Success
Connectivity OSPF Adjacency Failed Total occurrences: 850	<pre>IIIII Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms LA1-ASR1001X-2#</pre>	
Onboarding Wireless clients failed t Total occurrences: 48	> 2 Check OSPE neighbors	Run
Onboarding Wireless clients failed t Total occurrences: 48	 > 3 If the Neighbor is in "Init" state. Check if there is authentication configured using "show run sec 	DSPF".

Wireless Network Data Plane Categories



Wireless Network Data Plane Categories and Issues



Wireless Network Control Plane Categories



Ciscolive,

Wireless Network Control Plane Categories and Issues



Ciscolive!

Wireless Network Device Health Issues





Network Control Plane Issues



Network Data Plane Issues



Network Policy Plane Issues

ISE and access

- User policy instantiation failure due to not TCAM
- User policy instantiation failure due to SW failure on device



- Failed to communicate with controller (PXGRID problem) (1)
- Failure to download the destination list for access policy for SGT – Border (1) (Failed to install policy in Fabric border node)
- Failure to install an access policy for SGT (1) (Failed to install policy in Edge node)
- Failure to download access policy rules for SGT from ISE Edge (1)
- Failure to download the source list of access policy for SGT – Edge (1)
- Failure to uninstall an access policy for SGT (1)
- Failure to install an Ipv6 access policy for SGT (1)

Ciscolive!

Path Trace—Part 1 of 4

✓ Path Trace

To find the location of an issue, perform a path trace between two nodes in your network - a source device and a destination device.

10.30.100.27 (port: 8100) → 10.30.120.10 (port: 9100) [protocol: tcp] Jan 21, 2018 7:16 pm CAPWAP >0 +> >• ***** ** →• ***** →• (+* •-----. LA1-3-CSW-2 10.30.120.10 10.30.100.27 LA2-AP3802-23 LA2-3850-ACC-1 ... LA2-3850-CSW-3 LA1-3850-CSW-1 ... LA1-3850-CSW-2 ... LA1-WLC5520-2 LA1-3850-CSW-2... LA1-3850-CSW-1...

Run New Path Trace

Ciscolive!

Path Trace—Part 2 of 4 (Device Details and Stats)



Ciscolive

Path Trace—Part 3 of 4 (Interface Details and Stats)



Path Trace—Part 4 of 4 (QoS and ACL Stats)



PathTrace—How Does it Work?



Ciscolive!

BRKSDN-2777 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public 98

Application Health—Global

Ciscolive,



99

How Should Network App Treatment Quality be Measured?

A "service class" represents a set of traffic that **requires specific delay**, **loss**, **and jitter** characteristics from the network.

Conceptually, a service class pertains to applications with similar characteristics and performance requirements...

The 3 basic component metrics of Network Application Treatment Quality: Delay / Latency Jitter Loss



Application Experience—Client 360



All Applications ×

Filter

1 Export

Application		Health		Destination	Average	Average	QoS class-	DSCP	Path	:	
Name / IP	Port	Most Recent •	Last 24 hours	EAR-BRANN	Hate (mora)	ounzation	Ligross	markin	mace		
All Application		6		SEA	62	62%	<value></value>	AF41			
Webex / 192.23.11.4	40	4	\sim	SF	25	25%	«value»	AF31	00		
192.45.11.25	120	5		SF	92	92%	<value></value>	AF41	00		
119.192.4.16	44	5	~	PHX	73	73%	<value></value>	AF31	00		
File Transfer / 122.31.22.1	22	7		LA	92	92%	<value></value>	EF	00		
11.156.25.122	12	7	~	LA	92	92%	<value></value>	EF	00		





Calculating Jitter and Loss for RTP Apps





Calculating Jitter and Loss for TCP Apps



SND = Server Network Delay

CND = Client Network Delay

104

Troubleshooting Applications The Network vs. App Triage Decision



DNA Assurance / AppDynamics Integration



AppDynamics Dashboard and Insights



DNA Analytics and Assurance Techtorial

- The top-of-mind issue for most CIOs is digital transformation
- Most networking departments today are bogged down by operations, spending the majority of their time manually configuring and troubleshooting their networks
- Enabling an intent-based closed-loop architecture, including automation and analytics, significantly frees up IT time and resources
- This techtorial focused specifically on the role of analytics and assurance in the enterprise network architecture
- Client, Network and Application health monitoring, reporting and troubleshooting were all presented in-depth, as were additional use-cases of DNA Assurance.
- Additional ongoing-development initiatives were previewed, including Machine Learning, Application Integration (Skype-for-Business example) and Application Dynamics integration

Ciscolive,


Thank you



KSDN-2777 © 201

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public 109