Cisco live!

February 15 - 19, 2016 · Berlin, Germany

We’re ready. Are you?

DNS-AS-WRiedel-BRKSDN-3004-20160213-master.pptx

DNS-AS

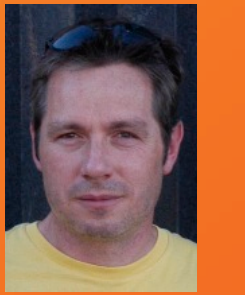
Done with SDN and
Tired of Dealing with Snowflake Network Complexity?
Change the Game with a Simple TXT String

Wolfgang Riedel

BRKSDN-3004

Wolfgang Riedel
Principal Engineer Engineering
ENG Product Management – Architecture
CCIE #13804, VCP #42559
wolfgang@cisco.com

Who is Wolfgang Riedel ???



- **Personal:**
  - Location: Erlangen, Germany (between Munich – Frankfurt)
  - Other Interests: Alpine Snowboarding, High-End Audio, AS51871, Data Center, Real World LAB, High-performance sports cars, Geothermal DC cooling research project, …

- **Background:**
  - Joined CISCO January 2001
  - Before; self-employed as an in-depended consultant in the Networking and IT space for more then fifteen years.
    - ✓ SE – RS Germany (2001 – 2006) -> Campus with a DC attached
    - ✓ CSE – DC EMEA (2006 - 2008) -> DC with Campus attached
    - ✓ CE – Cisco CTO Office (2008 – 2011)
    - ✓ PE – ARND (2011 – 2013)
    - ✓ PE – CTO Team ENG (2013 - 2014)
    - ✓ PE – Architecture Team ENG (2014 – …)
  - HA Campus & DC Design, Routed Access, DC POD Design
  - CCIE RS, VCP 3/4/5 and pile of CPOC's
  - Worked with more then 250 customers within several projects over the last +15 years
  - Individual Contributor: Cat4k, Cat6k, N7k, ASR1k, FC, FCoE, DCB, UCS, N5k, N2k, N1k, PoE FEX, vPC, OTV, LISP (Pioneer Award), OF, SDN

- **Stuff I am currently working on:**
  - Network Transformation, Architecture (Mark, Matthias, Tim, Dave, Jason, Simone, I)
  - APIC-EM, DNS-AS, AVC, USP
  - TECSDN-3600 + BRKCRS-3011 + BRKSDN-3004

Agenda

1. Introduction – What is DNS-AS
2. What is Network Metadata
3. Network Metadata within DNS RR's
4. How to manage "foreign" domains
5. DNS-AS Operations
6. Actually, what can we do with it?
7. DNS-AS Demo
8. Program Plans & Milestones
9. A Few Conclusions and Q&A, if we have time

Core Message:
Network Metadata

Warning:
A good portion of this session is about DNS
and DNS functionalities we use.
This is not about DNS-AS it's just supposed
to be a re-fresher for those of us which
forgot about it ;-)

1. Introduction
What is DNS-AS ???

Cisco live!

DNS-AS

Tenets of DNS-AS

Application Visibility

Today many applications operate in clear text and therefore it is possible to identify those by Deep Packet Inspection (DPI) methods on the network. How can you keep visibility if the majority of traffic is becoming encrypted?

Metadata Driven

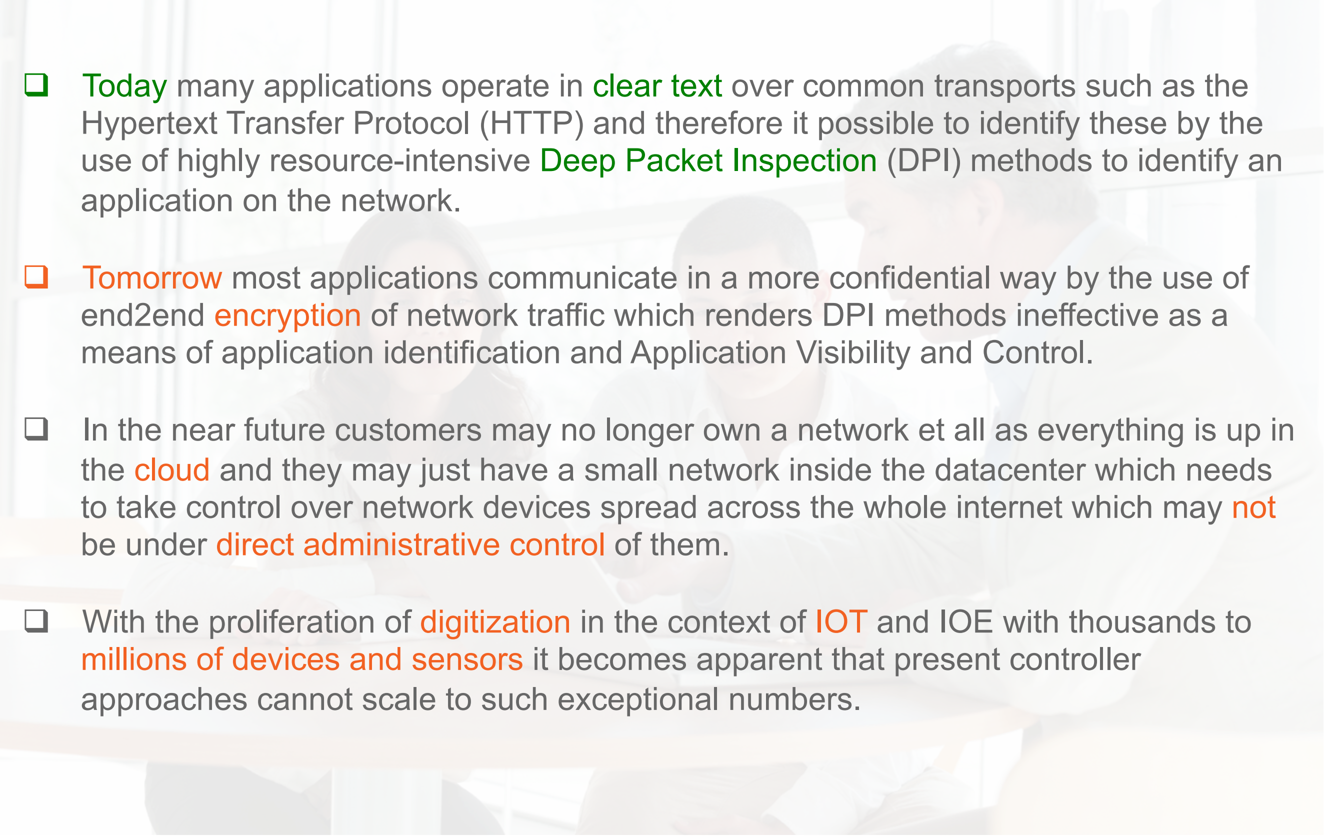
Metadata is information about applications that describes them. Instead of guessing device by device we holistically program the network via DNS-AS derived metadata no matter if the traffic is encrypted or not. Suddenly your network behaves like a self driving car.

Centralized Control

The Promise of OpenFlow and SDN had been “Decoupling Policy from Configuration” which resulted into a variety of SDN controllers. While the industry is busy trying to agree on something why not simply use the DNS infrastructure as a SDN controller?

DNS-AS

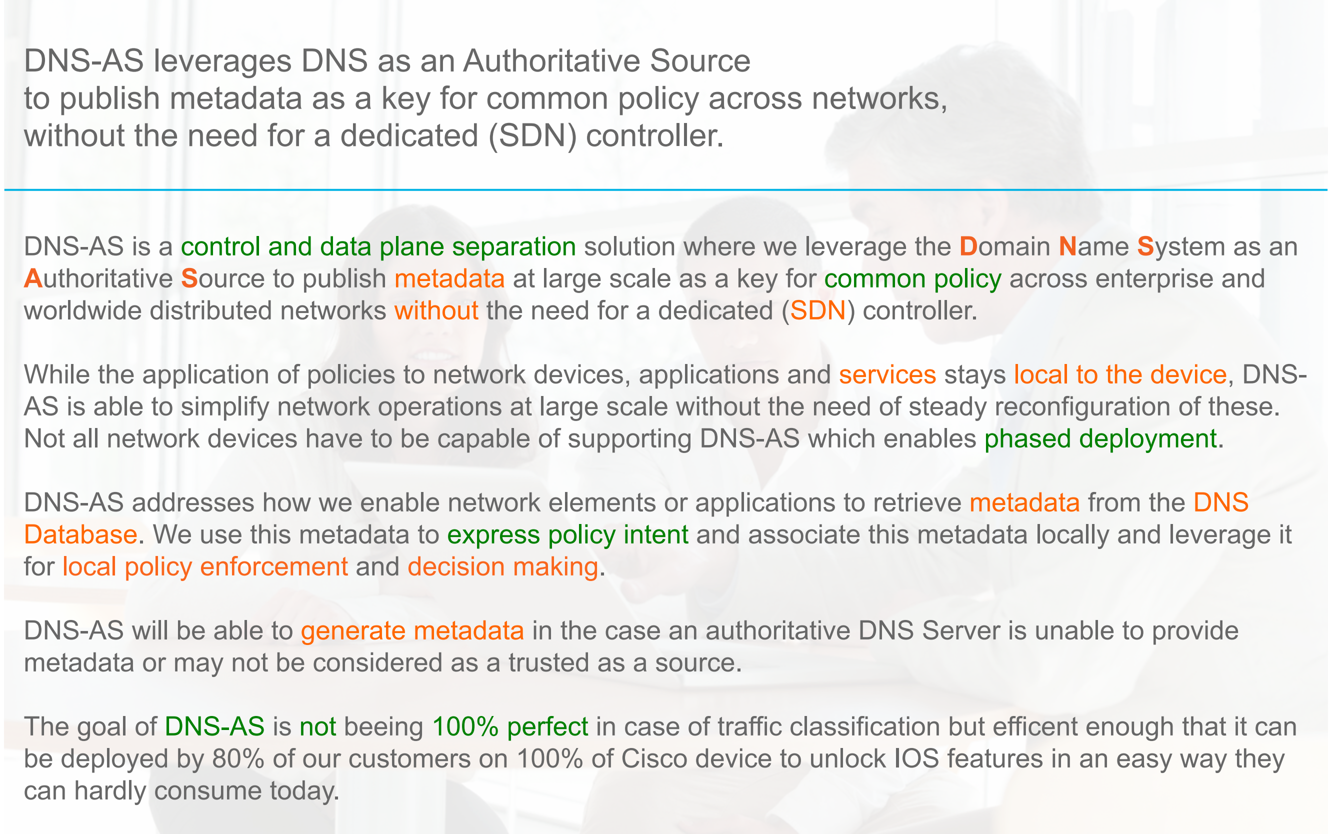
Problem Statement



- □ Today many applications operate in clear text over common transports such as the Hypertext Transfer Protocol (HTTP) and therefore it possible to identify these by the use of highly resource-intensive Deep Packet Inspection (DPI) methods to identify an application on the network.
- □ Tomorrow most applications communicate in a more confidential way by the use of end2end encryption of network traffic which renders DPI methods ineffective as a means of application identification and Application Visibility and Control.
- □ In the near future customers may no longer own a network et all as everything is up in the cloud and they may just have a small network inside the datacenter which needs to take control over network devices spread across the whole internet which may not be under direct administrative control of them.
- □ With the proliferation of digitization in the context of IOT and IOE with thousands to millions of devices and sensors it becomes apparent that present controller approaches cannot scale to such exceptional numbers.

DNS-AS

What is DNS-AS – The Burj Khalifa Elevator Pitch



DNS-AS leverages DNS as an Authoritative Source
to publish metadata as a key for common policy across networks,
without the need for a dedicated (SDN) controller.

DNS-AS is a control and data plane separation solution where we leverage the **D**omain **N**ame **S**ystem as an **A**uthoritative **S**ource to publish metadata at large scale as a key for common policy across enterprise and worldwide distributed networks without the need for a dedicated (SDN) controller.

While the application of policies to network devices, applications and services stays local to the device, DNS-AS is able to simplify network operations at large scale without the need of steady reconfiguration of these. Not all network devices have to be capable of supporting DNS-AS which enables phased deployment.

DNS-AS addresses how we enable network elements or applications to retrieve metadata from the DNS Database. We use this metadata to express policy intent and associate this metadata locally and leverage it for local policy enforcement and decision making.

DNS-AS will be able to generate metadata in the case an authoritative DNS Server is unable to provide metadata or may not be considered as a trusted as a source.

The goal of DNS-AS is not beeing 100% perfect in case of traffic classification but efficent enough that it can be deployed by 80% of our customers on 100% of Cisco device to unlock IOS features in an easy way they can hardly consume today.

1.1 SDN Industry Trends

Industry trends in Networking

Cloud (2008)

OpenFlow Networking (Stanford clean slate) (2011)

Software Defined Networking (2012)

OPEN DAYLIGHT
www.opendaylight.org

Open Daylight Project (2013)

DevOps, The API Driven Datacenter (2013)

Network Function Virtualization (2013)

Managing Networks through abstractions (2014)

Metadata Driven Networking (2016)

Atomic Services (2018)

SDN – Still Don't kNow – Stanford Defined Networking

The Promise of OF/SDN had been "Decoupling Policy from Configuration"

"An open solution for customized flow forwarding control in the Data-Center"

Physical separation of control and data plane

"A way to reduce the CAPEX of my network and leverage commodity switches"

"A platform for developing new control planes"

Managing the network through abstractions

"A way to avoid lock-in to a single networking vendor"

"With SDN I can develop solutions to my problems far faster –
"at software speeds" I don't have to work with my network
vendor or go through length standardization"

Whitebox routing and switching

"A means to do traffic engineering without MPLS"

"An open solution for VM mobility in the Data-Center"

Software Defined Networking

"A solution to build a very large scale layer-2 network"

"A means to scale my fixed/mobile gateways and optimize their placement"

Packet forwarding on x86 compute

"A solution to build virtual topologies with optimum multicast forwarding behavior"

"A way to define virtual networks with specific topologies for my multi-tenant Data-Center"

"A way to build my own security/encryption solution, avoiding RSA"

Running networks in agile DEV-OPS model

"A way to scale my firewalls and loadbalancers"

You can't just buy SDN.
It's an architecture which you have to embrace and life

"A way to configure my entire network as a whole rather than individual devices"

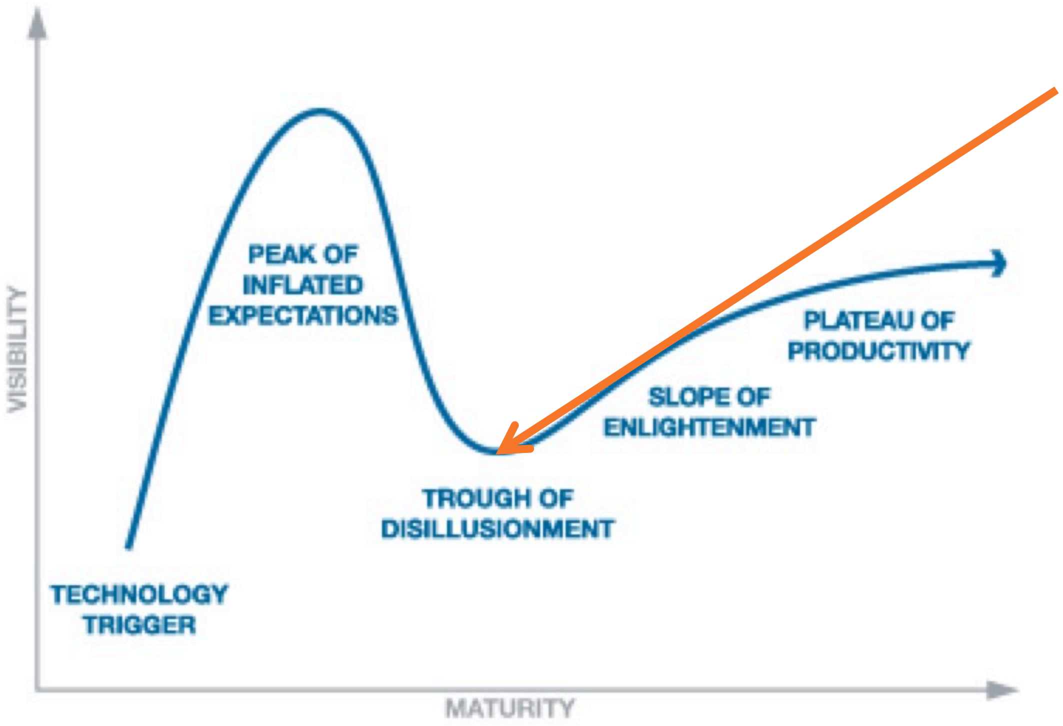
"A way to distribute policy/intent, e.g. for DDoS prevention, in the network"

"A way to optimize link utilization in my network through new multi-path algorithms"

"A solution to get a global view of the network – topology and state"

SDN – Hype Cycle

Where we are with SDN 2016, five years later



- Technology Trigger
- Peak of Inflated Expectations
- **Trough of Disillusionment**
  - Interest wanes as experiments and implementations fail to deliver.
  - Producers of the technology shake out or fail.
  - Investments continue only if the surviving providers improve their products to the satisfaction of early adopters.
- Slope of Enlightenment
- Plateau of Productivity

Gartner Hype Cycle

Managing the network through abstractions

There are two approaches to Control Systems

IMPERATIVE CONTROL

Baggage handlers follow sequences of simple, basic instructions

DECLARATIVE CONTROL

Air traffic control tells where to take off from, but not *how* to fly the plane

Managing the network through abstractions

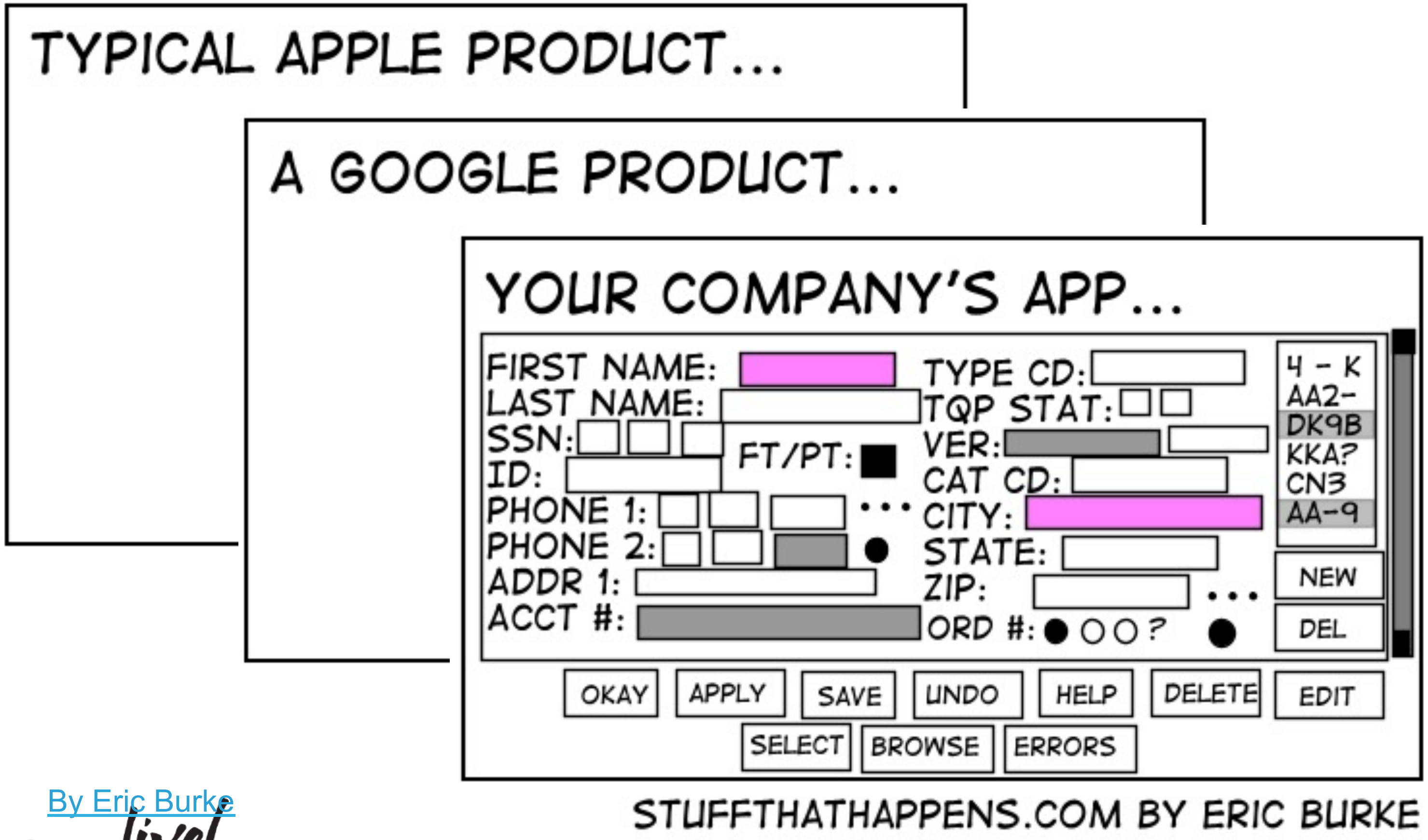
There are two approaches to Control Systems

IMPERATIVE CONTROL

DECLARATIVE CONTROL

It's 2016 and network admins still enjoy being "masters of complexity"

Enterprise SDN customer asks in an iPhone world



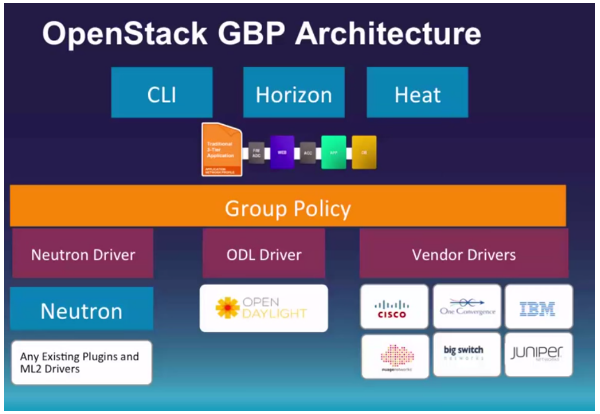
By Eric Burke

SDN Controllers – Types

There’s nothing like the SDN controller

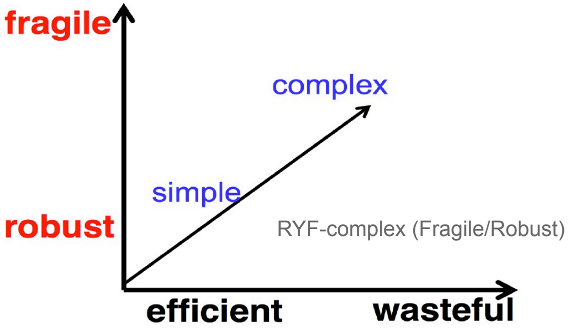
- SDN Config-Pusher
  - Orchestration (robot micromanaging manual to-do’s)
  - NCM (Network Configuration Management)
  - Customers may see or edit any part of the config
  - ✓ Prime Infrastructure, Action Packed, Solarwinds
  - ✓ Puppet, Chef
  - ✓ Openstack
  - ✓ Netconf
- SDN Policy-Compiler
  - Customer is never exposed to nor has access to nor influence over direct snippets of configuration elements.
  - They express their intent only – like in a programming language – and the conversion to machine language is invisible.
  - ✓ Cisco APIC-EM
- SDN Policy-Enabler
  - ✓ Cisco APIC-DC
- SDN Overlay Controller
  - ✓ VMWare: VCS, VCD, NSX
  - ✓ VSM (N1kv), EVP, VTS
  - ✓ Windows Server, Microsoft System Center)
- SDN Open Flow Controller
  - ✓ Primary for research

Group Based Policy / NIC



SDN Controllers – Types

Start with the End in Mind - the RYF-complex (Fragile/Robust)



Five dimensions of robustness in complex systems

(1) Reliability
(2) Efficiency
(3) Scalability
(4) Modularity
(5) Evolvability

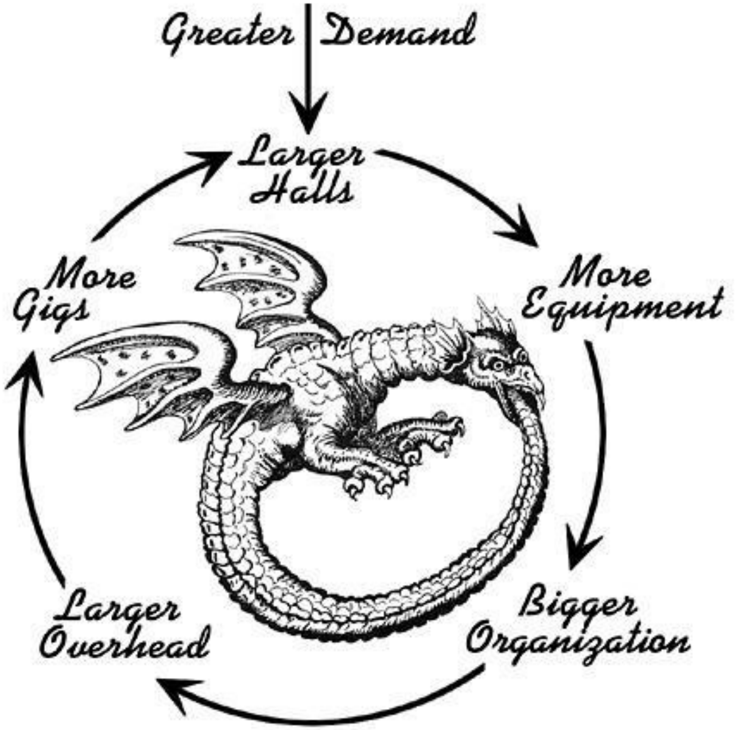
See J. Doyle, et. al.,
“Robustness and the Internet:
Theoretical Foundations”

Alderson and Doyle identify four kinds of constraints on system robustness:

(1) Component-level
(2) System-level
(3) Protocols
(4) Emergent constraints

Complex systems science as conflicting constraints
John C. Doyle, HOT and SF networks

Grateful Dead Sources
How the Dragon Urobouros (Giga Exponentia)
Makes Us Go Round and Round



How About DNS? – DNS server as a controller?

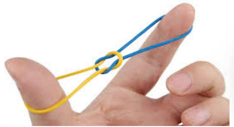
It's a pretty proven and awesome system, right?

Reliability

Using DNS - the most proven, used and scalable system of the Internet, to Distribute Metadata

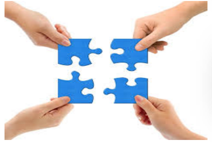
Efficiency

DNS well proven for it's efficiency – Light weight & Distributed with Tree Architecture



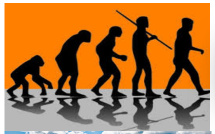
Scalability

DNS is a fully distributed system- scales well for the whole Internet!



Modularity

Decoupled DNS Network Infra and Agent running on Device (No endpoint requirements)



Evolvability

Has the capacity of Adaptive Evolution – Metadata not just limited to Network Devices

Performance

Hardware Acceleration possible – Potential for applications beyond QoS (security, etc …)

How About DNS Security? – Pretty Bad Privacy

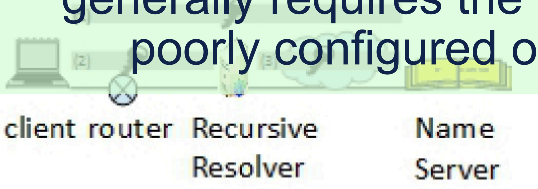
Threats: Monitoring and Surveillance (Haya Shulman, irtfopen @ IETF93)

DNS packets:

- Clear text is per se insecure (monitored, collected, logged)
- DNS data is public
- Research
- Operational purposes
- Financial gain: tailored ads
- Intelligence collection
- Censorship

Attackers:

- Eavesdroppers
- DNS/ networks operators
- Third party service providers
- URI dialing for VoIP (looking up phone number)



Privacy for DNS?

Large effort within research and operations communities to protect DNS privacy

- **Proposals (encryption most promising)**
  - DNSCurve / DNSCrypt
  - DNS over TLS
  - Opportunistic encryption
- **Differences**
  - What is protected
  - Channel vs DNS record
  - Adoption requirements
    - Changes to DNS message format
    - Changes to DNS software
    - New server port
    - Proposals for encryption assume support of TCP
- **Infrastructure compatibility, Protocol support**
  - Cloud providers: how to handle third party proxies?
  - Support of basic protocols : TCP, which version?
  - DNS and side channels: timing, sizes, domains dependencies, browsers' prefetching,…
- **DNSSEC for data integrity**
  - Singing DNS resource records using PKI

Question:

Is this really of concern for Enterprise Network?

DNS Data Integrity

Privacy ./. AVC

Security ./. User Experience

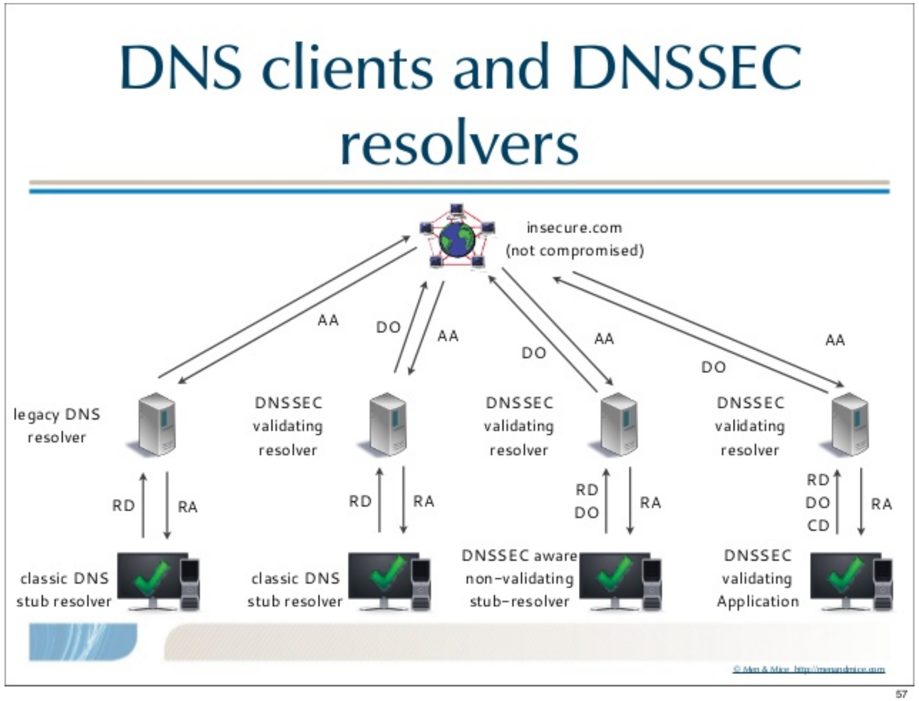
End2End Encryption ./. Company Policies

Security Audits?

DNS poisoning or spoofing, or similar vulnerabilities generally requires the attacker to take advantage of poorly configured or vulnerable DNS servers.

How About DNS Authenticity? – DNSSEC

Singing DNS resource records using PKI



DNS clients and DNSSEC resolvers

insecure.com
(not compromised)
AA
DO
AA
DO
AA
DO
AA
legacy DNS resolver
DNSSEC validating resolver
DNSSEC validating resolver
DNSSEC validating resolver
RD
RA
RD
RA
RD
DO
RA
RD
DO
CD
RA
classic DNS stub resolver
classic DNS stub resolver
DNSSEC aware non-validating stub-resolver
DNSSEC validating Application
© Men & Mice http://menandmice.com
57

- DNSSEC works by digitally signing each DNS record so that any tampering of that record can be detected.
- The digital signatures, and keys used to create them, are distributed just like any other records in the DNS making DNSSEC backward compatible.
- Keys in each layer in the DNS hierarchy are signed by keys from the preceding layer which effectively vouches for them just like domain names are delegated from one layer to the next.
- This "chain of trust" is used to validate the digital signatures accompanying DNSSEC protected records to detect changes.

How About Granularity?

Is DNS granular enough? - IP Address Explosion

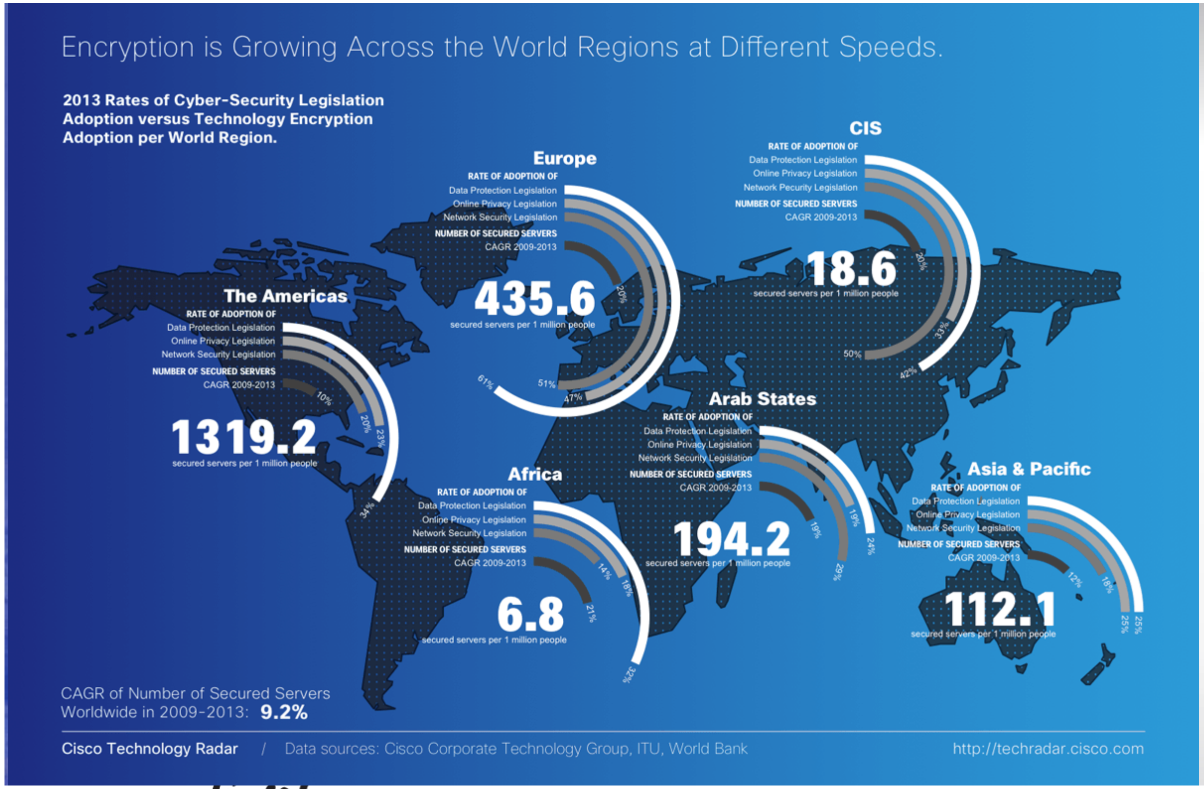
Networks continue to grow in size, importance, and complexity, organizations need to implement network services that are secure, scalable and fault tolerant

- One IP per service is the new norm
- IP Address Explosion:
  - VM Sprawl
  - M2M
  - My Own Private Internet
- IPv6 without DNS is impossible to manage
- DHCP makes the task of network configuration a breeze
- DNS is still key

1.2 Application and Protocol challenges

The World Two Years After “Snowden”

Growth of Encrypted Network Traffic

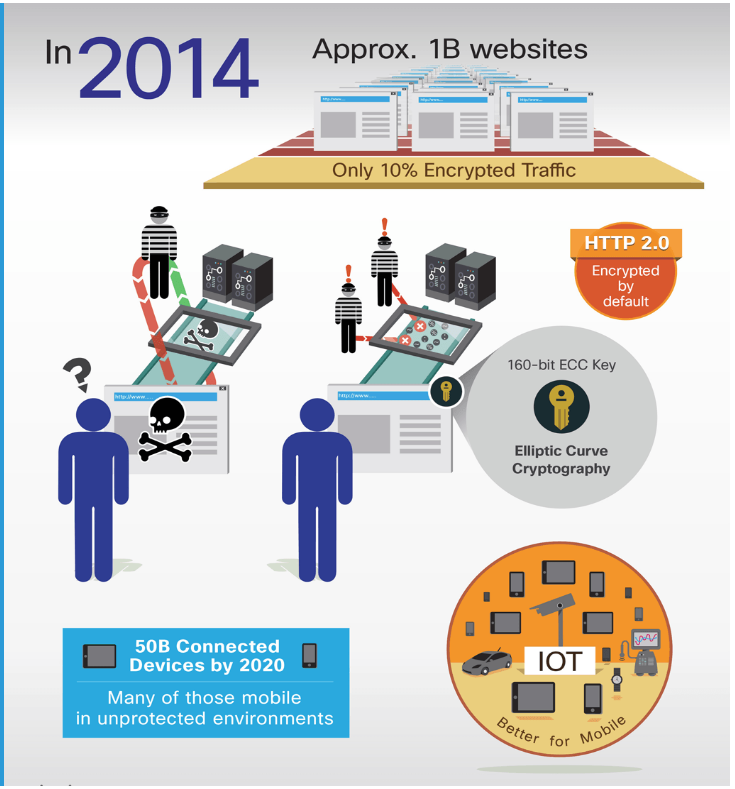

Encryption is Growing Across the World Regions at Different Speeds.

2013 Rates of Cyber-Security Legislation Adoption versus Technology Encryption Adoption per World Region.

The Americas
RATE OF ADOPTION OF
Data Protection Legislation
Online Privacy Legislation
Network Security Legislation
NUMBER OF SECURED SERVERS
CAGR 2009-2013
10%
20%
23%
34%
1319.2
secured servers per 1 million people
Europe
RATE OF ADOPTION OF
Data Protection Legislation
Online Privacy Legislation
Network Security Legislation
NUMBER OF SECURED SERVERS
CAGR 2009-2013
20%
51%
47%
61%
435.6
secured servers per 1 million people
CIS
RATE OF ADOPTION OF
Data Protection Legislation
Online Privacy Legislation
Network Pecurity Legislation
NUMBER OF SECURED SERVERS
CAGR 2009-2013
20%
50%
33%
42%
18.6
secured servers per 1 million people
Arab States
RATE OF ADOPTION OF
Data Protection Legislation
Online Privacy Legislation
Network Security Legislation
NUMBER OF SECURED SERVERS
CAGR 2009-2013
19%
29%
19%
24%
194.2
secured servers per 1 million people
Africa
RATE OF ADOPTION OF
Data Protection Legislation
Online Privacy Legislation
Network Security Legislation
NUMBER OF SECURED SERVERS
CAGR 2009-2013
21%
14%
18%
32%
6.8
secured servers per 1 million people
Asia & Pacific
RATE OF ADOPTION OF
Data Protection Legislation
Online Privacy Legislation
Network Security Legislation
NUMBER OF SECURED SERVERS
CAGR 2009-2013
12%
18%
25%
25%
112.1
secured servers per 1 million people

CAGR of Number of Secured Servers Worldwide in 2009-2013: **9.2%**

Cisco Technology Radar / Data sources: Cisco Corporate Technology Group, ITU, World Bank http://techradar.cisco.com



In 2014
Approx. 1B websites
Only 10% Encrypted Traffic
HTTP 2.0
Encrypted by default
160-bit ECC Key
Elliptic Curve Cryptography
50B Connected Devices by 2020
Many of those mobile in unprotected environments
IOT
Better for Mobile

The World Two Years After “Snowden”

Next-generation encryption - NSA-proof SSH

- Next-generation encryption efforts based on Elliptic Curve Cryptography (ECC) are promising. They provide the same level of encryption strength with shorter keys.
- The benefit is lower CPU consumption and low memory usage, two essential requirements for mobile devices such as sensors, actuators, controllers, and microcomputers, and the Internet of Things (IoT).
- As a result High Complex Encryption is becoming common and cheap

SSH version 1:
Ciphers: “blowfish”, “3des”, and “des”

SSH version 2:
Ciphers: aes256-gcm@openssh.com,aes128-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr

MACs: hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512

KexAlgorithms: curve25519-sha256@libssh.org,diffie-hellman-group-exchange-sha256

The World Two Years After “Snowden”

A tectonic shift for the Internet’s crypto landscape is coming

The current share of encrypted traffic on the web is largely due to Google, Facebook and Twitter, which have all by now adopted HTTPS by default.

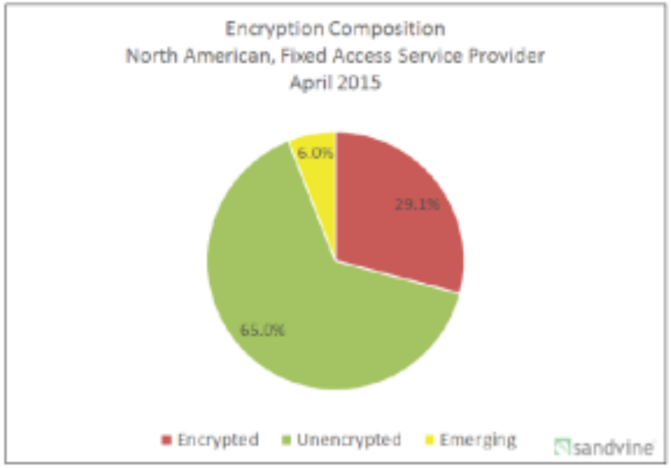


Figure 1 - Encryption Composition - North America, Fixed Access - April 2015

Netflix

- More than 40 million subscribers in the United States, about 60 million globally
- Accounts for more than a third of all downstream (or downloaded) north American Internet traffic
- “Over the next year we’ll evolve from using HTTP to using Secure HTTP (HTTPS) while browsing and viewing content on our service.
- This helps protect member privacy, particularly when the network is insecure, such as public WIFI, and it helps protect members from eavesdropping by their ISP or employer, who may want to record our members’ viewing for other reasons”

The World Two Years After “Snowden”

Let’s Encrypt is a new free Certificate Authority

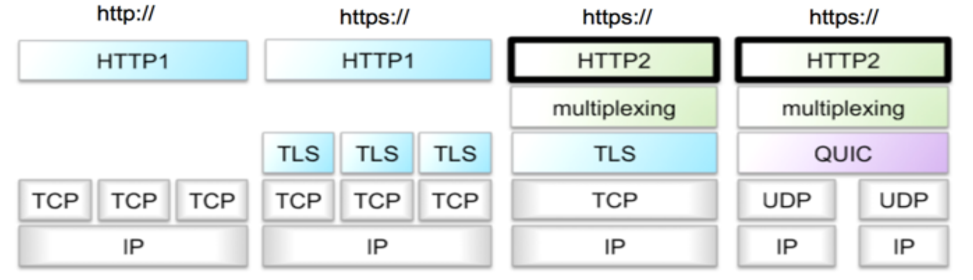
Let’s Encrypt

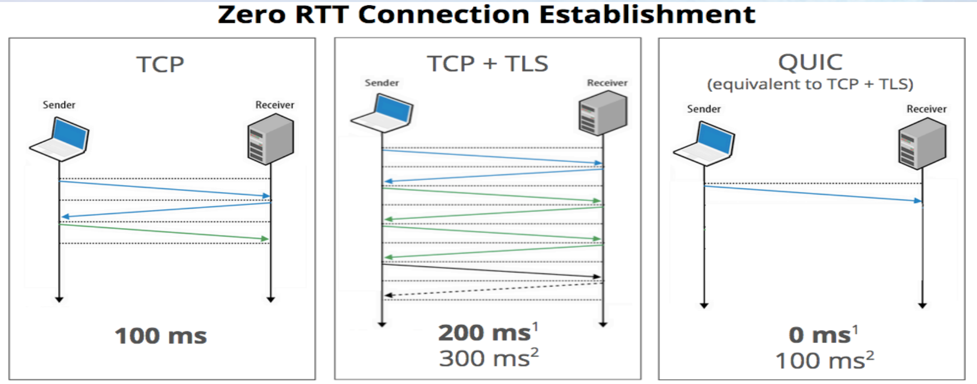
LINUX FOUNDATION COLLABORATIVE PROJECTS
mozilla
Akamai
CISCO
EFF
IdenTrust part of HID Global
AUTOMATTIC

Let’s Encrypt is a new Certificate Authority:
It’s free, automated, and open.

The World Two Years After “Snowden”

Protocol Evolution – HTTP/1, SPDY, QUIC, HTTP/2



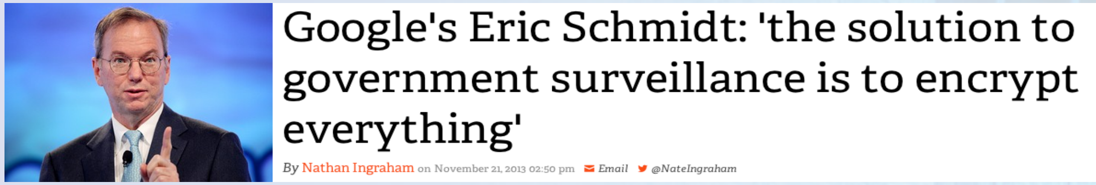


1. Repeat connection
2. Never talked to server before

- HTTP/1.0 was pioneered in the late 80’s
- HTTP/2 February 2015 IETF steering group announced completion
- Real performance improvement over TCP
- QUIC's lower-latency connection establishment
- zero-round-trip connection establishment
- TCP + TLS requires 2 to 3 round trips
- improved congestion control
- better loss recovery
- encryption capability by default

Living in a after “Snowden” world

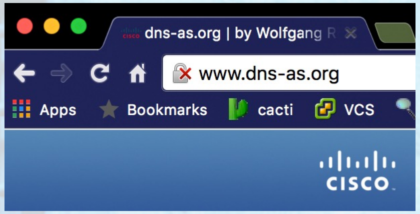
Google Will Soon Shame All Websites That Are Unencrypted - Motherboard



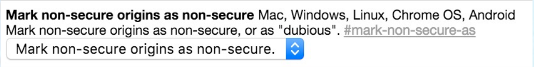
Google's Eric Schmidt: 'the solution to government surveillance is to encrypt everything'

By Nathan Ingraham on November 21, 2013 02:50 pm ✉ Email @NateIngraham

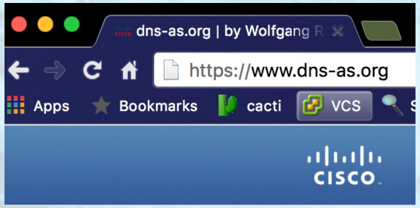
- Google wants everything on the web to be travelling over a secure channel.
- Future Chrome browser will flag unencrypted websites as insecure, displaying a red “x” over a padlock in the URL bar.
- “The goal of this proposal is to more clearly display to users that HTTP provides no data security.”
- **Google’s intention is to “call out” HTTP for what it is: “UNSAFE.”**



- Chrome: “chrome://flags”
- navigate to “mark non-secure as” and selecting “mark non-secure origins as non-secure.”

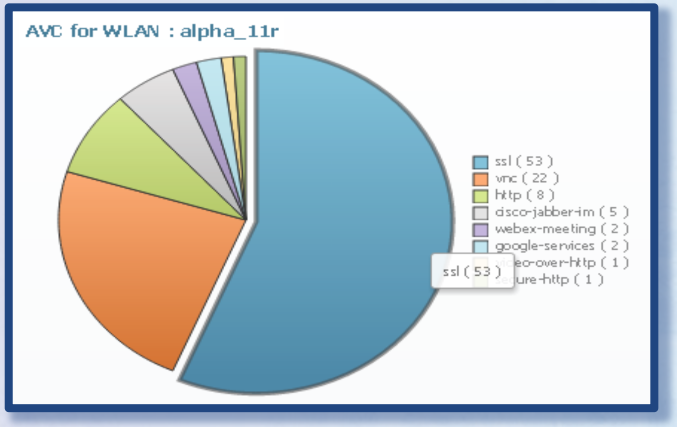


Mark non-secure origins as non-secure Mac, Windows, Linux, Chrome OS, Android
Mark non-secure origins as non-secure, or as "dubious". #mark-non-secure-as
Mark non-secure origins as non-secure.



Living in a after “Snowden” world

It becomes harder and harder for us to “guess”

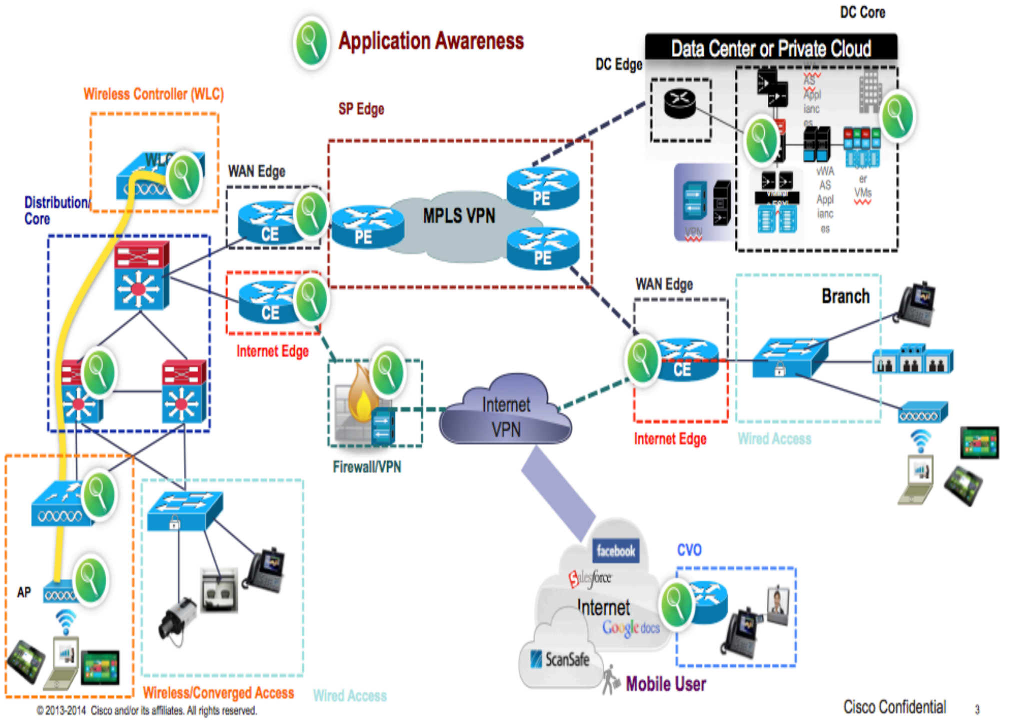


Bottom line: It becomes harder and harder for us to look into into traffic streams in order to “guess” what the apps are based on snooping traffic.

1.3 Evolution of AVC

AVC - Vision and Strategy

Network As a Sensor for Application Assurance



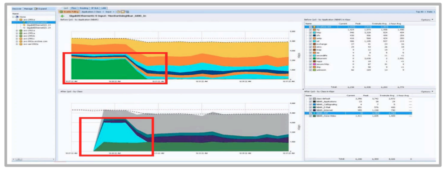
- Easy Deployment & Manageability of Applications in the Network
- Deliver Seamless Quality of Experience for Business Apps in the Network
- Drive SIMPLICITY - Abstract Network Complexity from Business Policies
- Lead with Flexible & Programmable Network Solutions in a fast-paced Application World

AVC - Use Cases

Know Applications (includes Growing Encrypted apps) In Your Network Granularly

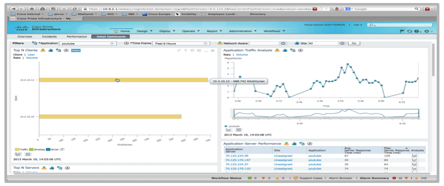
Needs Support across various PINS - Wireless, UA, WAN/Internet edge, Core, DC, Security

Business Level Policy Enforcement



E2E QoS & ACL (any Policy) enforcement – Drop "selectively", Access Marking & Core/ WAN Queuing

Application Level Reporting

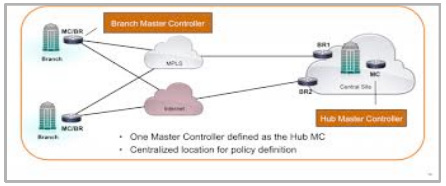


Visibility, Capacity Planning, Reporting on LAN & WAN

Network Data Analytics

Use Application Information to Drive Network Data Analytics – e.g. CMX/ wireless scenarios

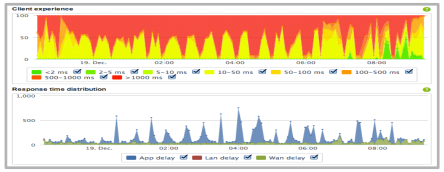
App-Aware "Domain Based" Routing



- One Master Controller defined as the Hub MC
- Centralized location for policy definition

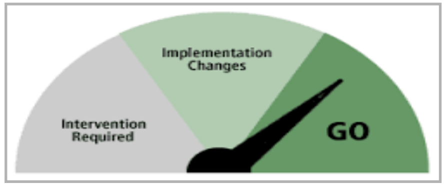
To support cloud apps breakouts to the Internet based on app-aware Routing policies

Application Level Troubleshooting & Easy Fault Isolation



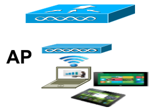
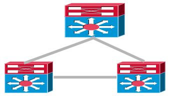
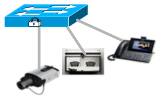
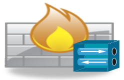
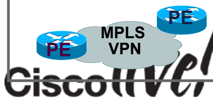
Zoom in on "Where The Problem Is" for business applications – could be ANYWHERE!

Network Readiness for Application Deployment



"Readiness Assessments" – Determine readiness for Application Deployment at planned scale

AVC – End to End – Why?

	**Wireless (WLC, AP), Converged Access**	2/3+ clients connect via wireless; Need to classify/mark at the edge; 90%+ still deploying centralized WLCs; Prevent scavenger apps from getting too deep! Block/Mitigate heavy hitters over shared (half duplex), second most congested medium!
	**Distribution, Core**	Troubleshooting – analyze traffic utilization (packet captures) Domain based routing starting at L3 Distribution for cloud apps (ITeS use case)
	WAN Edge	Premium Links & Limited Bandwidth – Need Capacity Planning & Optimal allocation for apps
	Internet Edge	Cloud migration – Need for DIA and first packet classification for cloud apps
	**Wired Access**	1/3 traffic still wired; 60-70% is voice/video with low latency requirements. Waiting till WAN is too late! Classification of this traffic known to be cumbersome today (port/subnet based)
	Data Center/Server Farm	Apps reside in DC – need to identify app level performance issues in multi-tiered client-server design
	**Firewall, Perimeter Security**	Entry Point (check what apps to allow) – Filter Applications/Users – URL filtering
	**MSP Edge**	Provide Application Level SLA – Managed Services

AVC – End to End – How?

Requirements for Future Application Identification:

We need an
Authoritative
Light-Weight
Unambiguous
way to identify applications.

We then need to be able to
link that Application Identity to Organizational Policy
for enforcement, accounting, etc.

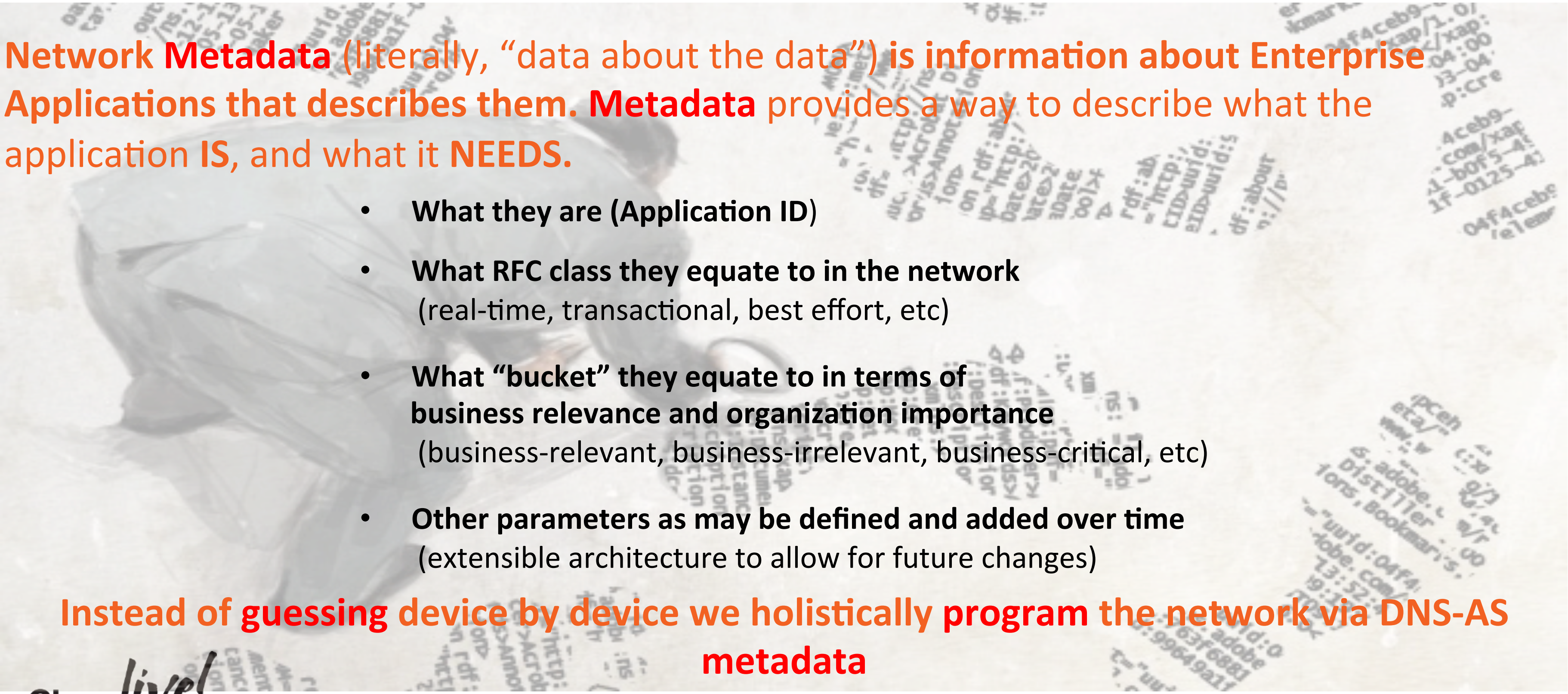
How can we do this while addressing the challenges noted?

Network Metadata

2. What is Network Metadata and how we integrate with existing technologies

Network Metadata – What is it? Why do we need it?

Definition of Metadata for Use



Network Metadata (literally, "data about the data") **is information about Enterprise Applications that describes them. Metadata** provides a way to describe what the application **IS**, and what it **NEEDS.**

- **What they are (Application ID**)
- **What RFC class they equate to in the network**
  (real-time, transactional, best effort, etc)
- **What "bucket" they equate to in terms of business relevance and organization importance**
  (business-relevant, business-irrelevant, business-critical, etc)
- **Other parameters as may be defined and added over time**
  (extensible architecture to allow for future changes)

Instead of guessing device by device we holistically program the network via DNS-AS metadata

Network Metadata – possible sources of truth

Multiple Application ID's out there

- Snort Open App ID
- SourceFire
- FireSIGHT eStreamer Application Protocol
- NBAR
- Meraki
- Simple Matches
- Application Information in IP Flow Information Export (IPFIX)
- AVC: Global Application ID assignment model http://www.rfc-editor.org/rfc/rfc6759.txt

Network Metadata strategy we have chosen for DNS-AS: RFC6759

Network Metadata – Components

RFC6759 Metadata Components

- General DNS-AS TXT record syntax: ‘CISCO-CLS=<option>:<val>{|<option>:<val>}*’
- Option-value pairs may appear in the same record, separated by a pipe character ‘|’.
- Example for such a TXT record with app metadata would be: "**CISCO-CLS=app-name:EXCHANGE**"

Important Supported Attributes:

1. Application Name
2. Traffic Class (QoS)
3. Business Relevance
4. Application ID (as in RFC 6759)

Optional Supported Attributes:

- ✓ Application Category
- ✓ Application Sub-Category
- ✓ Attributes (tunneled, encrypted, p2p)
- ✓ Server Port Range (to identify an application with ports)
- ✓ IP Protocol Specifier
- ✓ IP Version Specifier
- ✓ Min/Avg/Max Bandwidth consumption
- ✓ Max. Possible Packet Loss (in %)
- ✓ Max. Possible Jitter (in ms.)
- ✓ Max. Possible Latency (in ms.)
- ✓ Source of Metadata (NBAR2, DNS-AS server etc.)

Network Metadata – DNS-AS

RFC6759 Metadata Components mapping for DNS-AS Resource Records

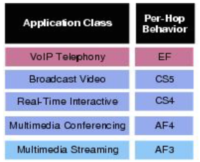
Attributes	Short Name	Comments
Application Name	**app-name**	**custom names are possible, minimum length to be 3 chars**
Application ID	**app-id**	**RFC 6759 based application ID names**
Application Category	app-category	
Application Sub-Category	app-sub-category	
Traffic Class (QoS)	**app-traffic-class**	**RFC 4594 based short names**
Business Relevance	**business**	**[YES|NO|DEFAULT]**
Next Hop	next	NSH - Service Chaining Next Hop
Attributes (tunneled, encrypted, p2p)	tunneled, encrypted, p2p	tunneled, encrypted, p2p
Server Port Range	port-range	to identify an application by ports
IP Protocol Specifier	ip-protocol	
IP Version Specifier	ip-version	
Min/Avg/Max Bandwidth consumption	min-bw, avg-bw, max-bw	
Max. Possible Packet Loss	max-pkt-loss	In %
Max. Possible Jitter	max-jitter	In ms
Max. Possible Latency	max-latency	In ms
Metadata derived from	source	NBAR2, DNS-AS-server, DNS-AS-proxy, RPZ

Network Metadata – Where to stuff these into?

RFC1035 Metadata Components

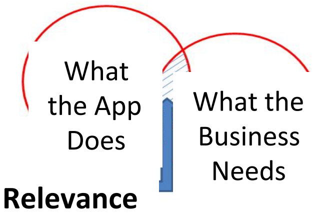
```
TXT RDATA format

    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    /                   TXT-DATA                      /
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+

TXT-DATA        One or more <character-string>s.
```

- TXT RRs are used to hold descriptive text. The semantics of the text depends on the domain where it is found.
- Originally for arbitrary human-readable text in a DNS record.
- Since the early 1990s, however, this record more often carries machine-readable data, such as specified by RFC 1464, opportunistic encryption, Sender Policy Framework, DKIM, DMARC, DNS-SD, etc.
- The base DNS specification limits DNS messages over UDP to 512 octets
- You can use multiple RRs, but this will make it complicated to sort the records



Application Class	Per-Hop Behavior
VoIP Telephony	EF
Broadcast Video	CS5
Real-Time Interactive	CS4
Multimedia Conferencing	AF4
Multimedia Streaming	AF3

- In general this kind of (ab)use of TXT RR is discouraged as discussed in RFC5507
- Historically, adding a new Resource Record Type has been very problematic. The review process has been cumbersome, DNS servers have not been able to handle new Resource Record Types, and firewalls have dropped queries or responses with Resource Record Types that are unknown to the firewall
- Today, there is a requirement that DNS software handle unknown Resource Record Types, and the approval process for new Resource Record Types has been updated [RFC5395] so the effort that is needed for various Resource Record Types is more predictable.
- Using TXT-RR is a short term approach to get something going and it’s working with all DNS servers out in the market
- **We want to get started NOW!**
- **Yes, we applied with IANA for a dedicated DNS-AS Resource Type Parameter Allocation (mnemonic = AVC)**



3. Network Metadata within DNS RR's

Network Metadata – BIND

```
$ORIGIN .
$TTL 3600       ; 1 hour
dns-as.org      IN SOA  ns1.f1-online.net. hostmaster.f1-online.net. (
                                2016020101 ; serial ; serial
                                14400      ; refresh (3 hours)
                                3600       ; retry (1 hour)
                                604800    ; expire (2 weeks)
                                3600       ; minimum (1 hour)
                                )
                        NS      ns2.f1-online.net.
                        NS      ns1.f1-online.net.
                        A       193.34.28.202
                        TXT     "CISCO-CLS=app-name:HTTP|app-class:TD"
                        MX      10 mx1.dns-as.org.
                        MX      10 mx2.dns-as.org.
                        TXT     "v=spf1 mx a ip4:193.34.28.0/24 ip4:193.34.29.0/24 ~all“
```

```
$ORIGIN dns-as.org.
assi                    A       193.34.28.205
                        TXT     "CISCO-CLS=app-name:ASSI|app-class:NC“
mail                    A       193.34.28.201
                        A       193.34.29.201
                        TXT     "CISCO-CLS=app-name:MX00|app-class:BD|business=yes"
mx1                     A       193.34.29.201
                        TXT     "CISCO-CLS=app-name:MX01|app-class:BD|business=yes"
mx2                     A       193.34.28.201
                        TXT     "CISCO-CLS=app-name:MX02|app-class:BD|business=yes"
ns1                     A       193.34.29.200
                        TXT     "CISCO-CLS=app-name:DNS-AS|app-class:OAM|business=yes"
ns2                     A       193.34.28.200
                        TXT     "CISCO-CLS=app-name:DNS-AS|app-class:OAM|business=yes"
sarav                   A       193.34.28.204
                        TXT     "CISCO-CLS=app-name:SARAV|app-class:NC"
wolfgang                A       193.34.28.203
                        TXT     "CISCO-CLS=app-name:WOLFGANG|app-class:OAM"
www                     A       193.34.28.202
                        TXT     "CISCO-CLS=app-name:DNS-AS-WWW|app-class:TD"
```

Network Metadata – How to verify

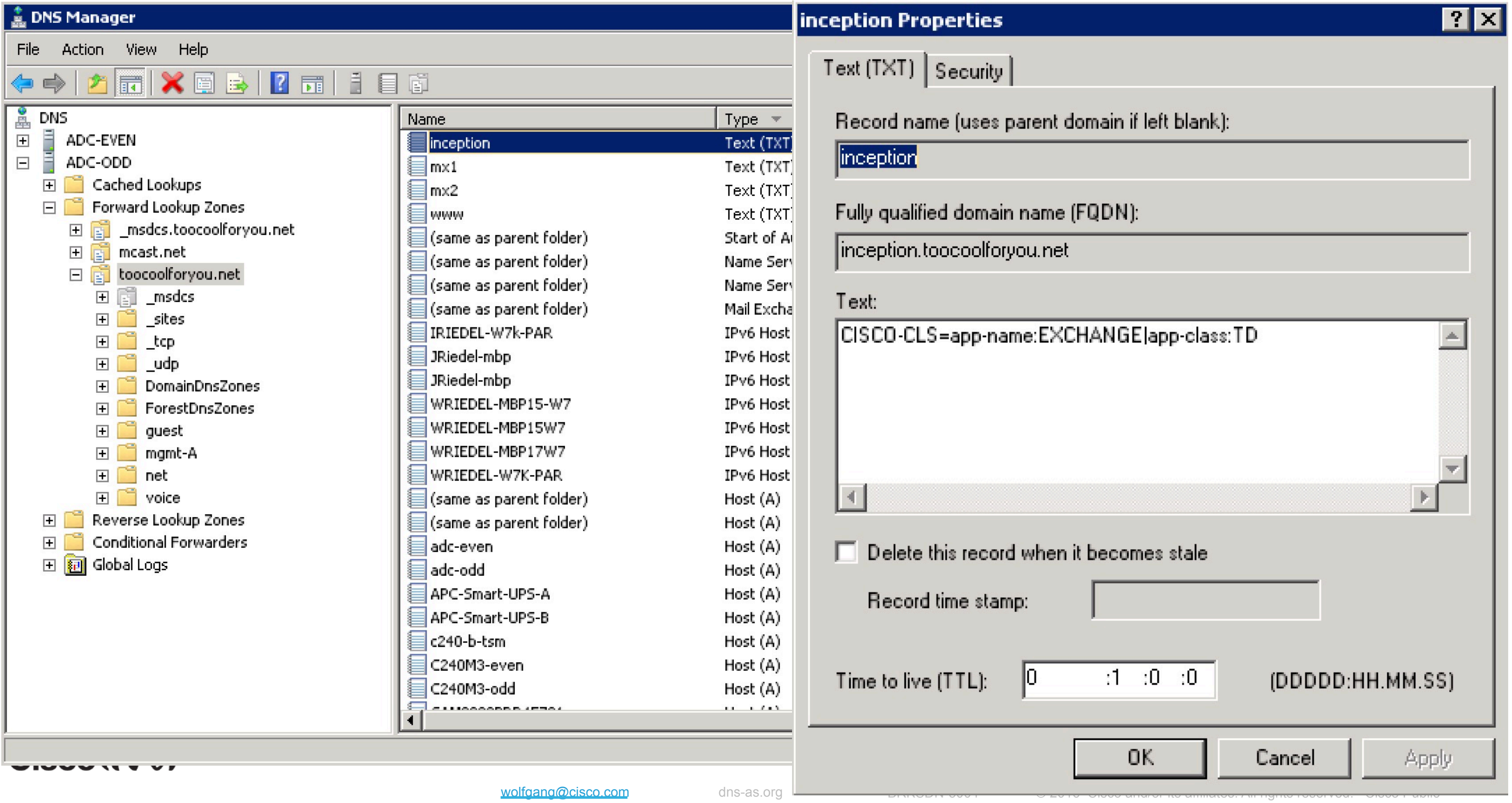
Forward Zone:

```
 [22:31:54][wriedel@wriedel-mbp15:~]$ dig TXT +short www.dns-as.org
"CISCO-CLS=app-name:HTTP|app-class:TD”

 [22:32:15][wriedel@wriedel-mbp15:~]$ dig TXT +short wolfgang.dns-as.org
"CISCO-CLS=app-name:WOLFGANG|app-class:OAM”

 [22:32:24][wriedel@wriedel-mbp15:~]$ dig TXT +short sarav.dns-as.org
"CISCO-CLS=app-name:SARAV|app-class:NC”

 [22:32:29][wriedel@wriedel-mbp15:~]$ dig TXT +short assi.dns-as.org
"CISCO-CLS=app-name:ASSI|app-class:NC”

 [22:32:38][wriedel@wriedel-mbp15:~]$ dig TXT +short inception.toocoolforyou.net
"CISCO-CLS=app-name:EXCHANGE|app-class:TD”
```

Reverse Zone:

```
 [22:31:40][wriedel@wriedel-mbp15:~]$ dig TXT +short 244.28.34.193.in-addr.arpa
"CISCO-CLS=app-name:DNS|app-class:BD”

 [22:31:41][wriedel@wriedel-mbp15:~]$ dig TXT +short 244.29.34.193.in-addr.arpa
"CISCO-CLS=app-name:DNS|app-class:BD”
```

Network Metadata – MS Active Directory



DNS
- ADC-EVEN
- ADC-ODD
  - Cached Lookups
  - Forward Lookup Zones
    - _msdcs.toocoolforyou.net
    - mcast.net
    - toocoolforyou.net
      - _msdcs
      - _sites
      - _tcp
      - _udp
      - DomainDnsZones
      - ForestDnsZones
      - guest
      - mgmt-A
      - net
      - voice
  - Reverse Lookup Zones
  - Conditional Forwarders
  - Global Logs

Name	Type
inception	Text (TXT
mx1	Text (TXT
mx2	Text (TXT
www	Text (TXT
(same as parent folder)	Start of A
(same as parent folder)	Name Serv
(same as parent folder)	Name Serv
(same as parent folder)	Mail Excha
IRIEDEL-W7k-PAR	IPv6 Host
JRiedel-mbp	IPv6 Host
JRiedel-mbp	IPv6 Host
WRIEDEL-MBP15-W7	IPv6 Host
WRIEDEL-MBP15W7	IPv6 Host
WRIEDEL-MBP17W7	IPv6 Host
WRIEDEL-W7K-PAR	IPv6 Host
(same as parent folder)	Host (A)
(same as parent folder)	Host (A)
adc-even	Host (A)
adc-odd	Host (A)
APC-Smart-UPS-A	Host (A)
APC-Smart-UPS-B	Host (A)
c240-b-tsm	Host (A)
C240M3-even	Host (A)
C240M3-odd	Host (A)

Record name (uses parent domain if left blank): inception

Fully qualified domain name (FQDN): inception.toocoolforyou.net

Text: CISCO-CLS=app-name:EXCHANGE|app-class:TD

☐ Delete this record when it becomes stale

Record time stamp:

Time to live (TTL): 0 :1 :0 :0 (DDDDD:HH.MM.SS)

Enterprise IP Address Management

Vendor	Deployment Modes Supported	DNS/DHCP Services Supported
Alcatel-Lucent	Integrated, Management Overlay, Managed Services	BIND, Microsoft and self-branded
BlueCat	Integrated, Management Overlay, Managed Services	BIND, Microsoft, Internet Systems Consortium (ISC) DHCP and self-branded
BT	Integrated, Management Overlay, Managed Services	BIND, Microsoft, ISC DHCP, Cisco Network Registrar (CNR) and self-branded
Cisco	Integrated, Management Overlay, Managed Services	BIND, Microsoft, ISC DHCP and self-branded
EfficientIP	Integrated, Management Overlay, Managed Services	Name server daemon (NSD), Unbound, BIND, Microsoft, ISC DHCP, Amazon Web Services (AWS) Route 53 and self-branded
FusionLayer	Integrated, Management Overlay	ApplianSys, BIND, Microsoft, ISC DHCP, Unbound, NSD, Nominum, Secure64 and self-branded
InfoBlox	Integrated, Management Overlay, Managed Services. The DNS engine is based on BIND 9 (with enhancements). Add providers or manage your own list with a GUI	BIND, Microsoft, ISC DHCP, F5 Global Traffic Manager (GTM) and self-branded
Men & Mice	Integrated, Management Overlay	BIND, Microsoft, ISC DHCP, Unbound, Cisco IOS, AWS Route 53 and PowerDNS
Microsoft	Integrated	Microsoft
SolarWinds	Management Overlay	BIND, Microsoft, ISC DHCP and Cisco IOS
ISC	CLI	BIND 9

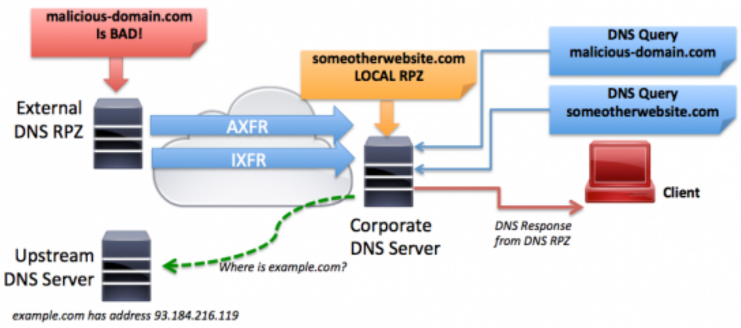
Source: Gartner (February 2015)

4. How to control “foreign” domains

DNS Firewall Response Policy Zones (RPZ)

BIND Response Policy Zones

- Most modern electronic crime and network abuse relies on the Domain Name System (DNS)
- A DNS firewall can selectively intercept DNS resolution for known-malicious network assets including domain names, IP addresses, and name servers.
- Interception can mean rewriting a DNS response to direct a web browser to a "walled garden", or simply making the malicious network assets invisible and unreachable.
- **Requires BIND 9.10 + but how about Windows ???**



A response policy in DNS RPZ can be matched as follows:

- by the query name
- by an address which would be present in a truthful response
- by the name or address of an authoritative name server responsible for publishing the original response.

A response policy action can be one of the following:

- to synthesize a "domain does not exist" response
- to synthesize a "name exists but there are no records of the requested type" response.
- to replace the response with specified data.
- to exempt the response from further policy processing.

DNS Firewall dnsrpz.info

Providers of reputation data	Service	Services Supported
DissectCyber	rpzone.us	
FarsightSecurity	Newly Observed Domains and example	
InternetIdentity	DNS firewall	
SpamHaus	Several of their popular blocklists are available via RPZ. Article Pricing	
SURBL	Data Feed	
ThreatStop	DNS firewall and announcement	
SecurityZones	Provider	Provides product marketing and sales for some of the providers above
Deteque	Provider	Has provided integration consulting for some of the DNS RPZ providers above
OpenDNS		Integrated, Management Overlay, Managed Services

Comparison of DNS blacklists

RPZ - configuration

```
options { forward first;
          forwarders {
                208.67.222.222; // opendns.org
                208.67.220.220; // opendns.org
                8.8.8.8; //google-public-dns-a.google.com.
                8.8.4.4; //google-public-dns-b.google.com.
                };
        response-policy { zone "rpz.f1-online.net"; zone "rpz.spamhaus.org"; zone "rpz.surbl.or
"rpz.ph.surbl.org"; }; };
```

```
zone "rpz.f1-online.net”    { type slave; file "rpz.f1-online.net.zone"; masters { 193.34.28.244; 193.34.29.244; }; check-names ignore; };
zone "rpz.spamhaus.org"     { type slave; file "dbl.rpz.spamhaus.org.zone"; masters { 199.168.90.51; 199.168.90.52; 199.168.90.53; };
zone "rpz.surbl.org"        { type slave; file "rpz.surbl.org.zone"; masters { 94.228.131.210; 94.228.131.211; }; check-names
zone "rpz.mw.surbl.org"     { type slave; file "rpz.mw.surbl.org.zone"; masters { 94.228.131.210; 94.228.131.211; };
zone "rpz.ph.surbl.org"     { type slave; file "rpz.ph.surbl.org.zone"; masters { 94.228.131.210; 94.228.131.211; };  check
```

1. response-policy option

2. local RPZ slave zone

3. remote RPZ slave zone’s

named.conf

```
[…]
; return NXDOMAIN for facebook.com
www.facebook.com            666      CNAME .
*.facebook.com              666      CNAME .

; redirect to walled garden IP’s
www.badguys.org     666     A        10.10.10.1
*.badguys.org               A        10.10.10.1
rpz.dns-as.org              A        10.0.2.21
wolfgang.cisco.com          A        193.34.28.108

; do not rewrite www.cisco.com (so, PASSTHRU) but add or override DNS-AS metadata
www.cisco.com               CNAME    rpz-passthru.
*.cisco.com                 CNAME    rpz-passthru.
www.cisco.com               TXT      "CISCO-CLS=app-name:HTTP|app-class:TD”
*.cisco.com                 TXT      "CISCO-CLS=app-name:HTTP|app-class:TD”

; rewrite A and add DNS-AS metadata
www.bradreese.com        A           72.163.4.161
www.bradreese.com        TXT         "CISCO-CLS=app-name:HTTP|app-class:SCV”
```

4. local RPZ master zone DNS-AS overrides

CNAME rpz-passthru. would be great but does not work, today

A + TXT works today

rpz.f1-online.net

DNS - Summary

DNS, as it's today already gives us a bunch of options

- Don't fix what's not fundamentally broken, don't develop a new protocol and controller for every new use case, utilize what we already use today
- We can assume that DNS really scales well, right ;-)
- Incremental steps
- RPZ allows us to fix others shortcomings (forward and reverse)
- How about DNS Security?
  - OK, don't let me get started on that one ;-)
  - Follow Best Practice's
  - If DNS is screwed we have a much bigger problem
  - VRF's
  - Autonomic Networking (self-managed PKI + ACP)
  - DNSSEC
  - MACSEC
  - BIND-CHROOT, SE-linux
  - Split DNS: MS AD, DMZ RR's, DMZ AS
  - Did I already mention, follow Best Practice's

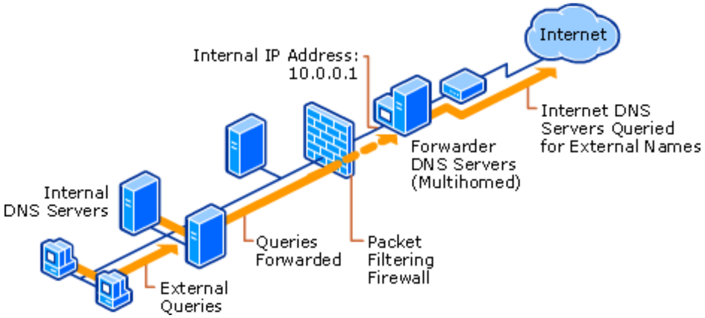
5. DNS-AS Operations

BIND and DNS

What Constitutes an Authoritative Source

The BIND software distribution has three parts:

- Domain Name Resolver
- Domain Name Authority server
- Tools


Internet
Internal IP Address: 10.0.0.1
Internet DNS Servers Queried for External Names
Forwarder DNS Servers (Multihomed)
Internal DNS Servers
Queries Forwarded
Packet Filtering Firewall
External Queries

Domain Name Authority server

- An authoritative DNS server answers requests from resolvers, using information about the domain names it is authoritative for
- There can just be ONE ZONE being authoritative per domain

Domain Name Resolver

- A resolver is a program that resolves questions about names by sending those questions to appropriate servers and responding appropriately to the servers' replies.
- In the most common application, a web browser uses a local stub resolver library on the same computer to look up names in the DNS. That stub resolver is part of the operating system.
- The stub resolver usually will forward queries to a caching resolver, a server or group of servers on the network dedicated to DNS services. Those resolvers will send queries to one or multiple authoritative servers in order to find the IP address for that DNS name.

The DNS-AS Acronym Decoder Ring

Split-DNS

An enterprise typically has different authoritative servers for internal and external clients, and publish some zones on the internal servers only.

- ✓ Internal zones, managed from an Active Directory
- ✓ External zones, managed from a single ‘master’ BIND system (DMZ)
- ✓ Caching recursive resolvers for “external” domains (DMZ)

Response Policy Zones

RPZ is a BIND mechanism to selectively override foreign zones we are not authoritative for

DNS-AS-RR

A DNS TXT record inside a forward or reverse ZONE file

TXT "CISCO-CLS=app-name:HTTP|app-class:TD”

DNS-AS-client (Enterprise: client -> application server)

A client side Network Element running a DNS stub resolver for resolving DNS-AS-RR by using the client DNS request as a trigger for a forward lookup with a fallback to a reverse lookup

DNS-AS-client (Datacenter: application server -> client)

An application server side Network Element running a DNS stub resolver for resolving DNS-AS-RR by using the application IP as a trigger for a reverse lookup

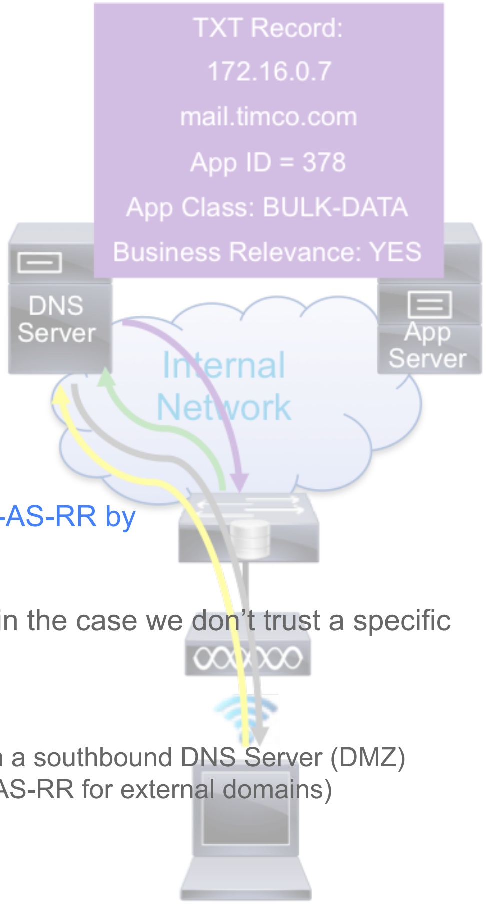
DNS-AS-proxy

Inserts metadata (DNS-AS-RR) in case not being provided by a northbound DNS server or in the case we don’t trust a specific domain (malware, porn,…)

DNS-AS-edge

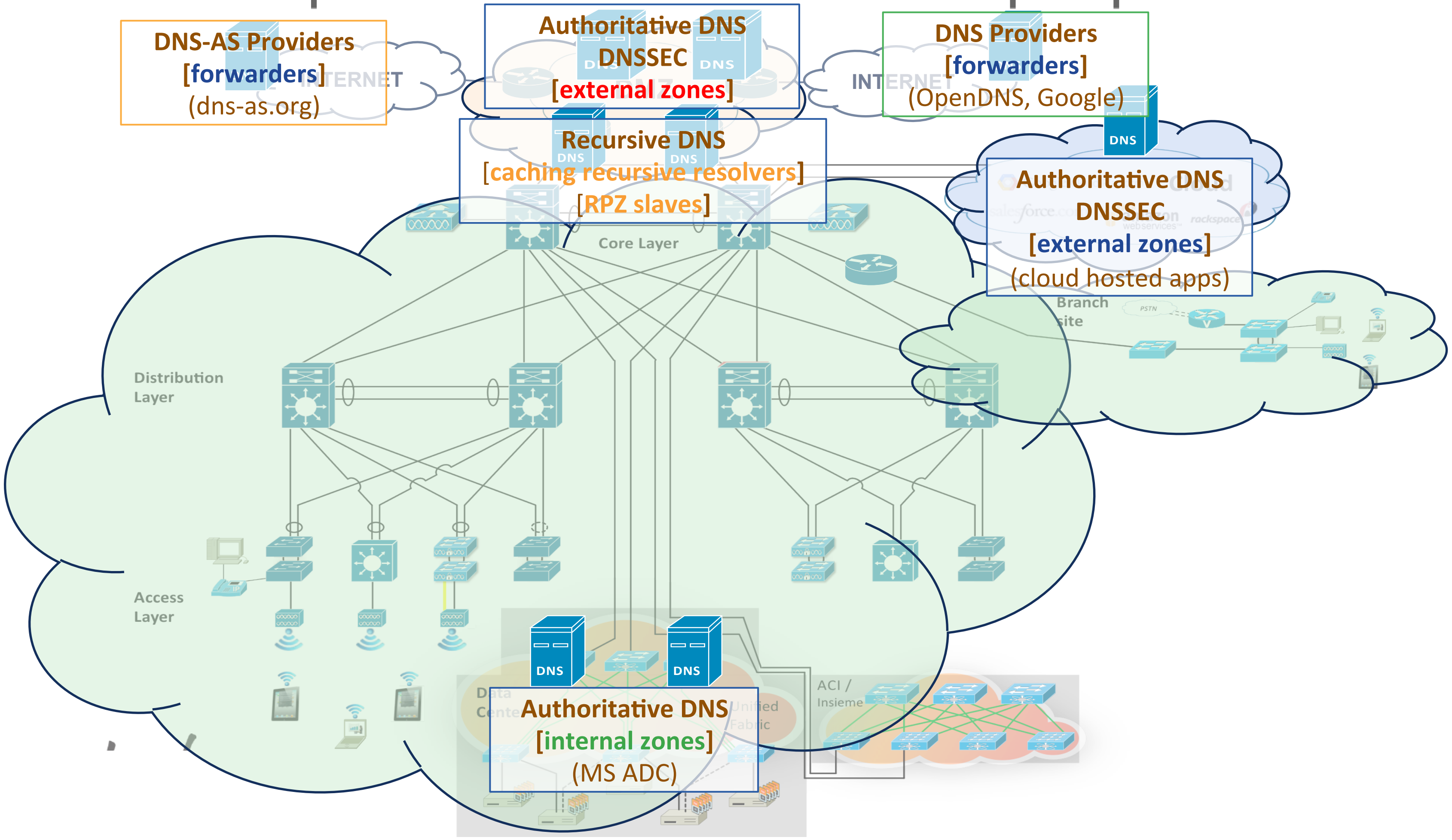
Internet facing Border Routers running two DNS-AS functions

- ✓ DNS-AS-client (even if running a DNS-AS-proxy on the same box) derives it's DNS-AS-RR from a southbound DNS Server (DMZ)
- ✓ DNS-AS-proxy (ensures that the southbound DNS servers (DMZ BIND) have meaningful DNS-AS-RR for external domains)



TXT Record:
172.16.0.7
mail.timco.com
App ID = 378
App Class: BULK-DATA
Business Relevance: YES

In an Enterprise - DNS lives in multiple places



DNS-AS Providers
[forwarders]
(dns-as.org)

Authoritative DNS
DNSSEC
[external zones]

DNS Providers
[forwarders]
(OpenDNS, Google)

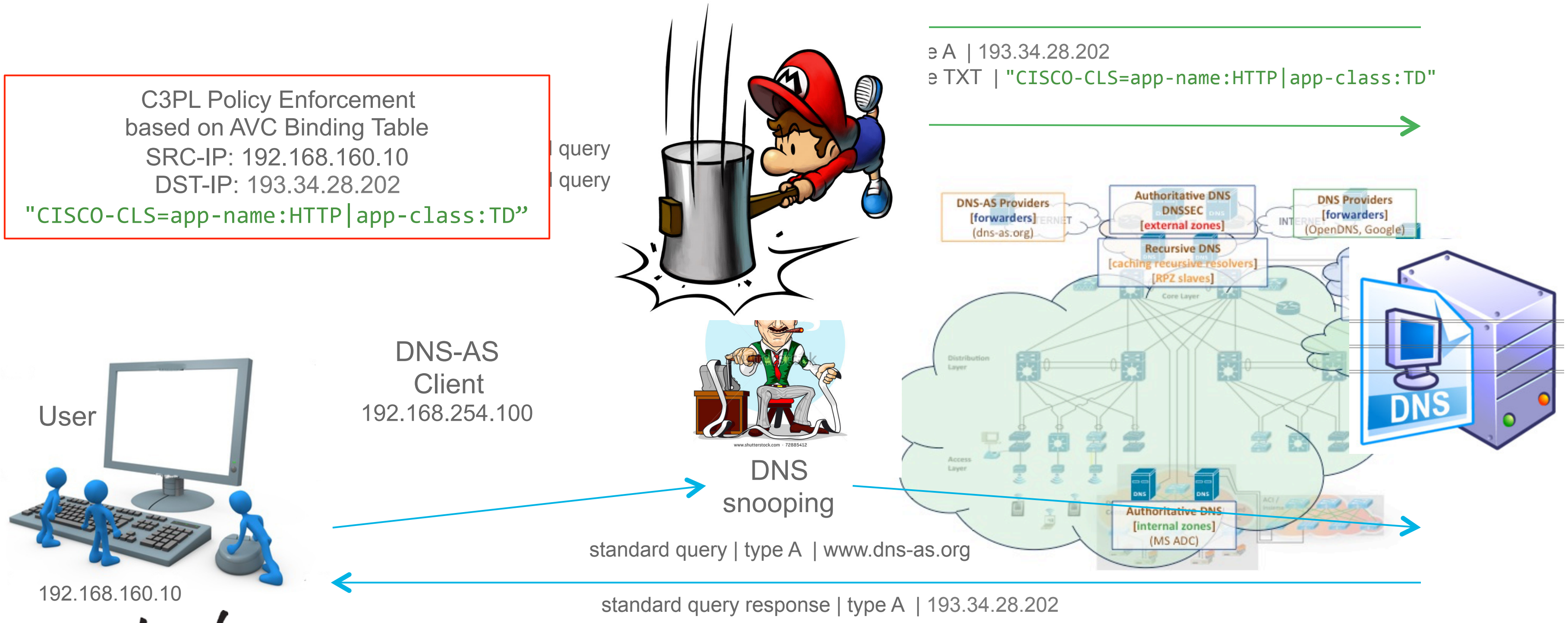
Recursive DNS
[caching recursive resolvers]
[RPZ slaves]

Authoritative DNS
DNSSEC
[external zones]
(cloud hosted apps)

Authoritative DNS
[internal zones]
(MS ADC)

DNS-AS-Client - Operations

DNS-AS Client (APs, Switches, Routers)



e A | 193.34.28.202

e TXT | "CISCO-CLS=app-name:HTTP|app-class:TD"

C3PL Policy Enforcement
based on AVC Binding Table
SRC-IP: 192.168.160.10
DST-IP: 193.34.28.202
"CISCO-CLS=app-name:HTTP|app-class:TD”

query

query

User

192.168.160.10

DNS-AS
Client
192.168.254.100

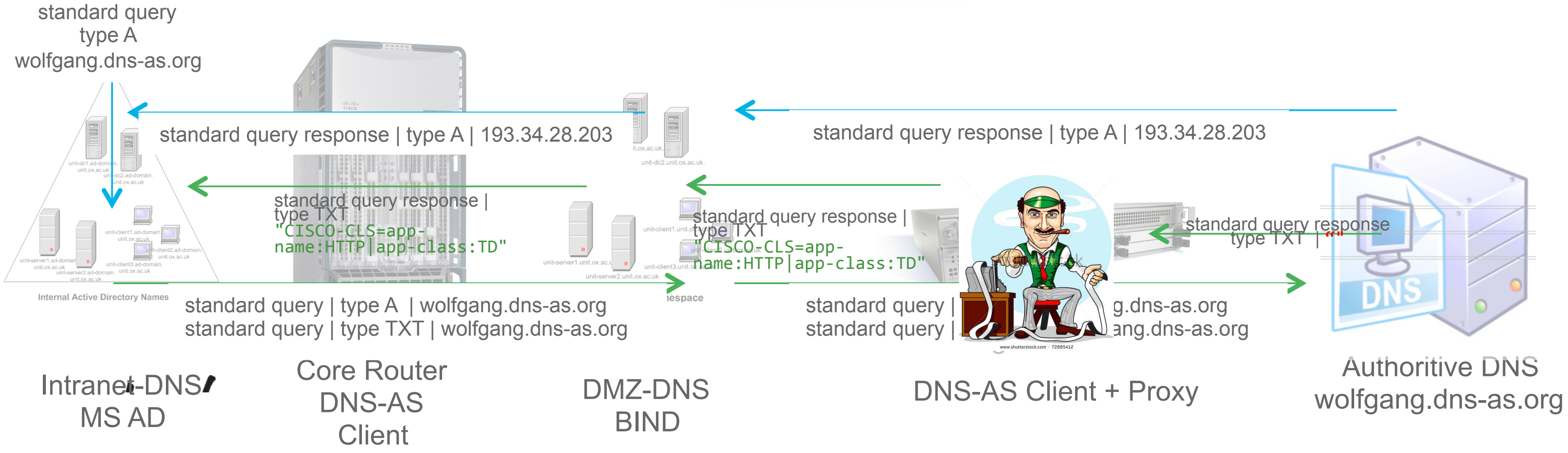
DNS
snooping

standard query | type A | www.dns-as.org

standard query response | type A | 193.34.28.202

DNS-AS-Proxy - Operations

Inline packet injection, after a DNS-AS client request



standard query
type A
wolfgang.dns-as.org

standard query response | type A | 193.34.28.203

standard query response | type A | 193.34.28.203

standard query response |
type TXT
"CISCO-CLS=app-name:HTTP|app-class:TD"

standard query response |
type TXT
"CISCO-CLS=app-name:HTTP|app-class:TD"

standard query response
type TXT | “”

standard query | type A | wolfgang.dns-as.org
standard query | type TXT | wolfgang.dns-as.org

standard query | g.dns-as.org
standard query | ang.dns-as.org

Intranet-DNS
MS AD

Core Router
DNS-AS
Client

DMZ-DNS
BIND

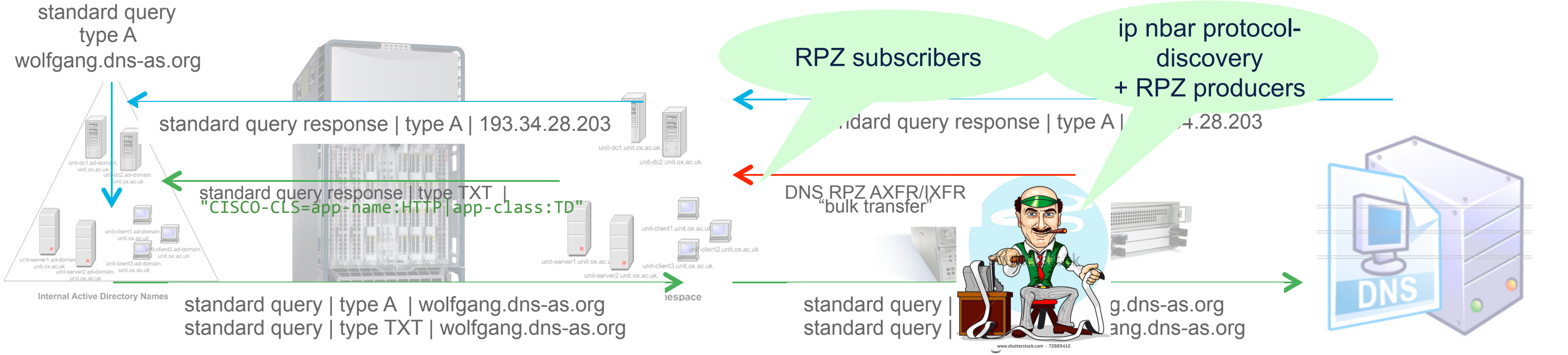
DNS-AS Client + Proxy

Authoritive DNS
wolfgang.dns-as.org

unit-dc1.ad-domain.unit.ox.ac.uk
unit-dc2.ad-domain.unit.ox.ac.uk
unit-client1.ad-domain.unit.ox.ac.uk
unit-client2.ad-domain.unit.ox.ac.uk
unit-client3.ad-domain.unit.ox.ac.uk
unit-server1.ad-domain.unit.ox.ac.uk
unit-server2.ad-domain.unit.ox.ac.uk
Internal Active Directory Names
it.ox.ac.uk.
unit-dc2.unit.ox.ac.uk.
unit-server1.unit.ox.ac.u
unit-server2.unit.ox.ac.uk.
unit-client1.unit.ox.ac.uk
unit-client3.unit.ox.ac.uk
iespace
DNS
www.shutterstock.com · 72885412

DNS-AS-Proxy - Operations

RPZ Zone Transfer DNS-AS-Proxy Router to DNS-AS-Server


standard query
type A
wolfgang.dns-as.org
standard query response | type A | 193.34.28.203
standard query response | type TXT |
"CISCO-CLS=app-name:HTTP|app-class:TD"
standard query | type A | wolfgang.dns-as.org
standard query | type TXT | wolfgang.dns-as.org
Internal Active Directory Names
RPZ subscribers
ip nbar protocol-discovery
+ RPZ producers
ndard query response | type A | 4.28.203
DNS RPZ AXFR/IXFR
"bulk transfer"
standard query | g.dns-as.org
standard query | ang.dns-as.org
DNS

Intranet-DNS,
MS AD

Core Router
DNS-AS
Client

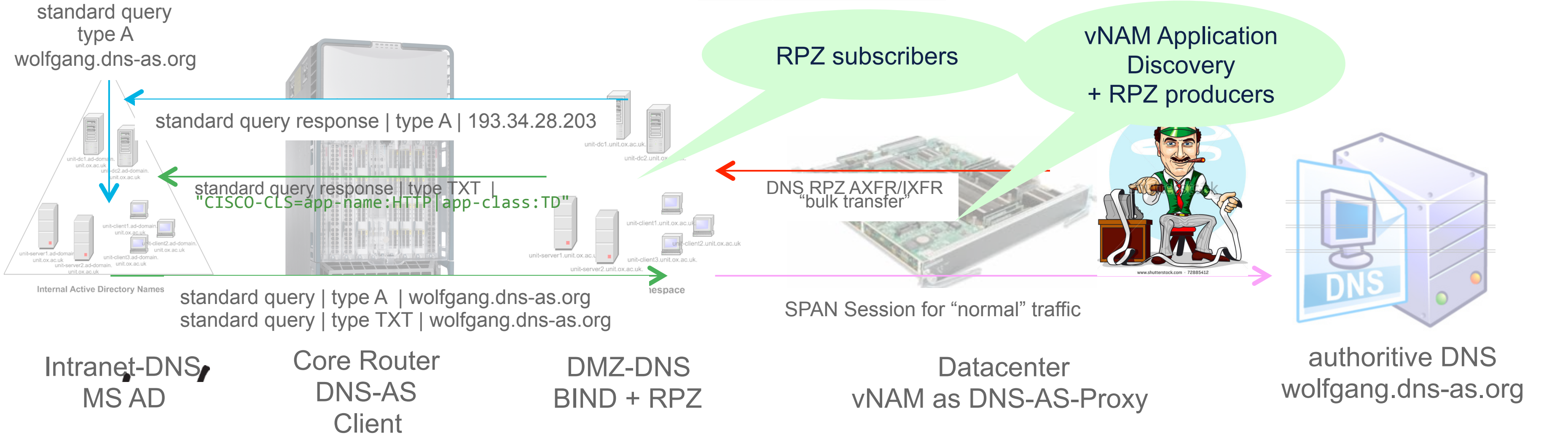
DMZ-DNS
BIND + RPZ

DNS-AS Client + Proxy

authoritive DNS
wolfgang.dns-as.org

DNS-AS-Proxy - Operations

RPZ Zone Transfer DNS-AS-Proxy vNAM to DNS-AS-Server



standard query
type A
wolfgang.dns-as.org

standard query response | type A | 193.34.28.203

standard query response | type TXT |
"CISCO-CLS=app-name:HTTP|app-class:TD"

standard query | type A | wolfgang.dns-as.org
standard query | type TXT | wolfgang.dns-as.org

RPZ subscribers

vNAM Application
Discovery
+ RPZ producers

DNS RPZ AXFR/IXFR
"bulk transfer"

SPAN Session for "normal" traffic

Intranet-DNS,
MS AD

Core Router
DNS-AS
Client

DMZ-DNS
BIND + RPZ

Datacenter
vNAM as DNS-AS-Proxy

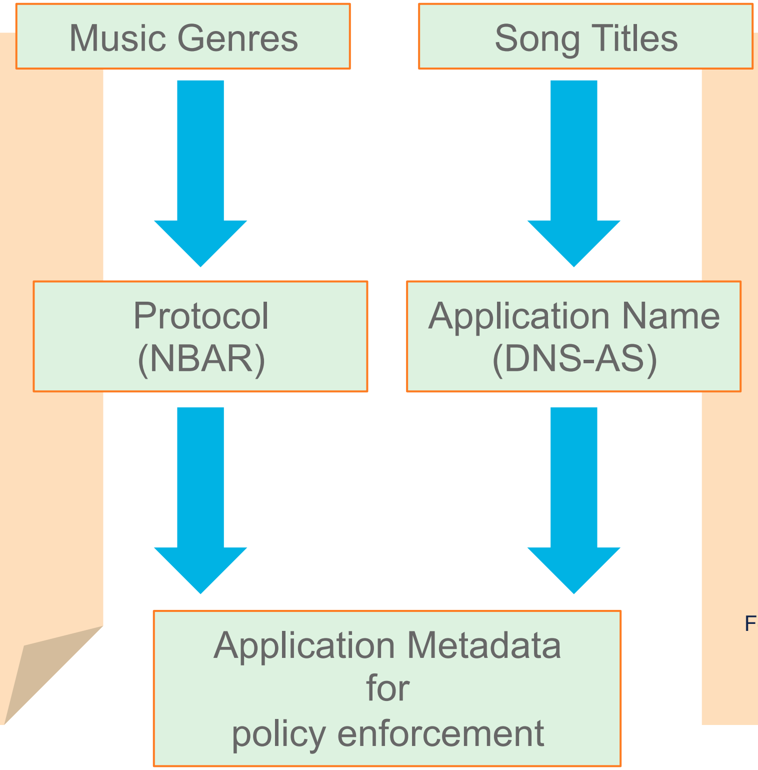
authoritive DNS
wolfgang.dns-as.org

6. Actually, what can we do with it?

DNS-AS ./. NBAR Different Solutions for Different Problems

How do you “play” your favorite song?

Alternative Music
Blues
Classical Music
Country Music
Dance Music
Easy Listening
Electronic Music
European Music (Folk / Pop)
Hip Hop / Rap
Indie Pop
Inspirational (incl. Gospel)
Asian Pop (J-Pop, K-pop)
Jazz
Latin Music
New Age
Opera
Pop (Popular music)
R&B / Soul
Reggae
Rock
Singer / Songwriter (inc. Folk)
World Music / Beats



I See Fire, Addal
Pray, Avery
I Loved You, Blonde Feat. Melissa Steel
How Deep Is Your Love, Calvin Harris & Disciples
Ayo
Help Me Lose My Mind, London Grammar
Hot Right Now, Rita Ora
Hotline Bling, Drake
Aint Nobody, Feat. Jasmine Thompson
Unter Meiner Haut, Gestört Aber Geil
Take Me To Church,   Hozier
I See Fire, asmine Thompson
Thinking Out Loud, Jasmine Thompson
Wide Awake, Katy Perry
This Is How We Do, Katy Perry
Interlude, London Grammar
All Eyes On You, Meek Mill
Stolen Dance, Milky Chance
Lieblingsmensch, Namika
Wrapped Up, Olly Murs
Wish You Were Mine, Philip George
Do It Again, Pia Mia
FourFiveSeconds, Rihanna and Kanye West and Paul McCartney
Sun Goes Down, Robin Schulz
Money On My Mind, Sam Smith

URL parsing ./. DNS-AS Metadata

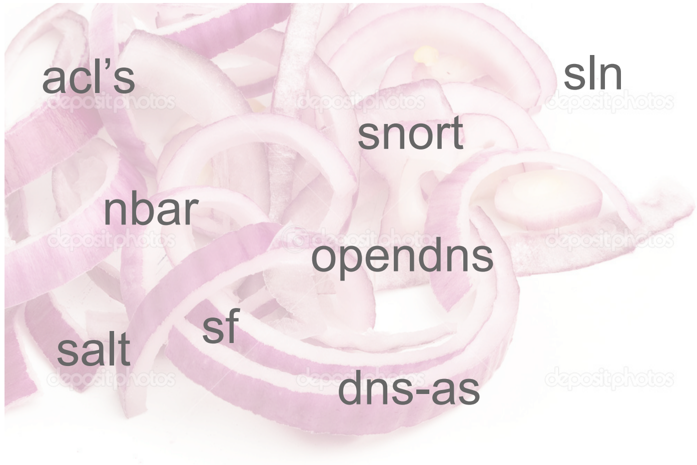
A much less expensive way to achieve 80% of the goal

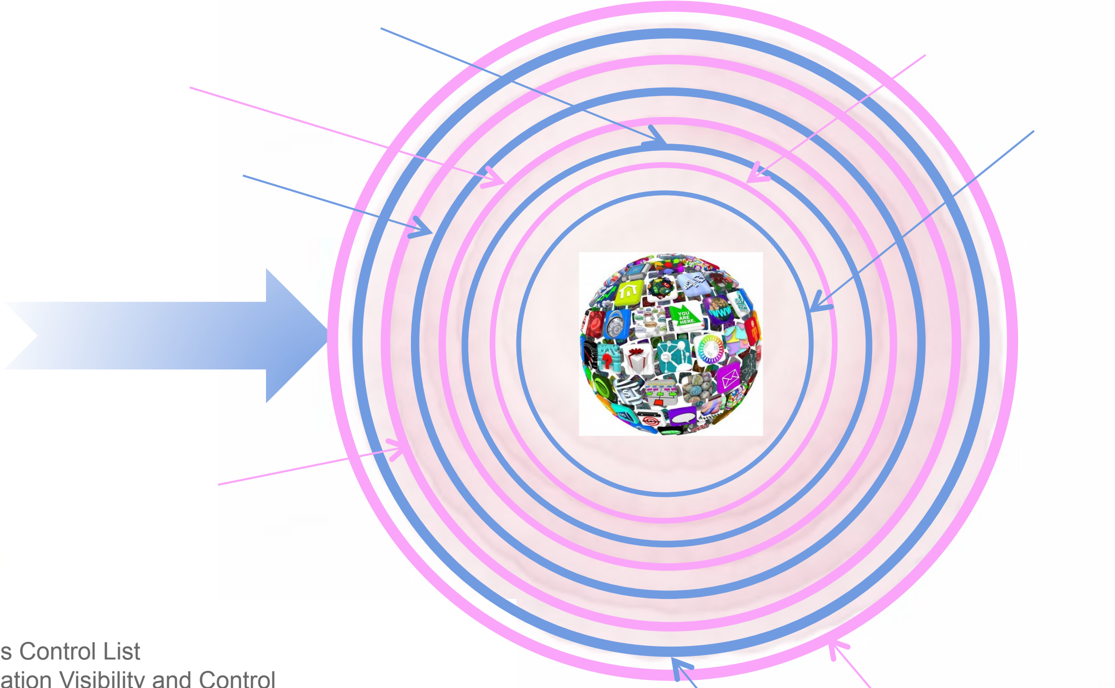
Keep it
SIMPLE
STUPID

```
http://username:password@www.dns-as.org:443/path/file.name?query=string#anchor

{
       scheme: "http://"
       user: "username",
       password: "password",
       host: "www.dns-as.org",
       port: "8080",
       path: "/path/file.name",
       query: "?query=string",
       fragment: "#anchor”
}
```

- As of today to we need to parse the whole URL to get application specific granularity
- At a fraction of the cost in terms of CPU and Hardware requirements you get similar results
- You get 80% of the goal for 100% consistency
- From a technical feasibility point of view a key enabler for common policy across our product portfolio

The AVC Multilayer Onion Ring Architecture





Acronym Decoder Ring:

/acl/	Access Control List
/avc/	Application Visibility and Control
avc/r	
avc/c	
avc/s	
avc/s	
avc/s	
/avc/sf	Source Fire
/avc/opendns	opendns.org

1. Principle: **Protection**
The outer layer protects the inner layer

2. Principle: **Declarative Control**
Don't spend cycles trying to learn or guess what you can program

3. Principle: **Power of AND**
It's not about one is better then…
We need them all!

AVC Network Metadata order of operation

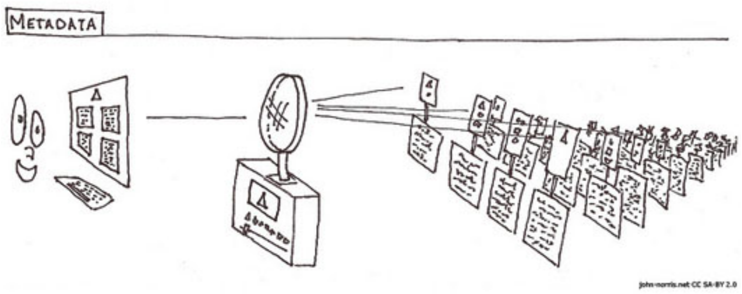
Admin Distance for AVC

- We started with a routing like admin distance approach
- Current approach is to make the AVC Engine super intelligent so no manual interaction is needed
- DNS-AS derived metadata has priority over NBAR built-in signatures.

1. Flow based signaling
   a. E.g. DPI learned a bundled flow for FTP-data or for RTP
   b. E.g. Media flows learned from direct server/client metadata
2. L3/4 Custom protocols
3. Local DNS-AS override and locally defined DNS based custom protocols
4. Custom DPI signatures
5. Regular, Protocol Pack based DPI signatures
6. Last-resort/generic, Protocol pack based DPI signatures, including statistical etc.

Common AVC Library – DNS-AS Use Case Matrix

Everywhere you want to match on Metadata



john-norris.net CC SA-BY 2.0

- Reporting via FNF even if encrypted
- Easy QoS
- Troubleshooting
- SPAN
- Martian ACL’s
- IPSLA
- Domain Based Routing
- ZBF (Zone Based Firewalls)
- NSH (Service Chaining)

Common AVC Library – DNS-AS Use Case Matrix

RFC6759 <metadata> as a variable to match within C3PL MQC

```
1) QoS
         class-map match-all NETWORK-CONTROL
          match protocol attribute traffic-class network-control
          match protocol attribute business-relevance business-relevant
          match protocol <metadata>
```

```
2) Zone Based Firewalls
         class-map type inspect match-all class-in-ssh
          match access-group name ACL-IPv4-ssh-in
          match protocol ssh
          match protocol <metadata>
```

```
3) Security ACL’s
         ip access-list extended ACL-IPv4-Minecraft-in
          remark ----- minecraft.f1-online.net ———
          permit tcp any host 193.34.29.143 eq 25565
          permit protocol <metadata>

         ip access-list standard ACL-IPv4-NMS
          remark ----- NOC DMZ
          permit aaa.bb.ccc.ddd
          permit protocol <metadata>
          remark ---- deny everything else --------
          deny   any log
```

```
4) Object Group
         object-group service port-proxy-server
          tcp eq 8080
          match protocol <metadata>
```

```
5) Domain Based Routing
         track 104 match protocol <metadata>
         ip route 192.168.168.0 255.255.255.0 192.168.252.114 111 track 104
```

Common AVC Library – Easy QoS Integration

DNS-AS Shortcuts for Cisco’s (RFC 4594-Based) 12-Class QoS Model

APPLICATION CLASS	APPLICATION CLASS long	APPLICATION CLASS short	BUSINESS-RELEVANCE	DSCP	COS	WMM	QUEUING & DROPPING	APPLICATION EXAMPLES
(RFC 4594)	DNS-AS-RR (LONG)	DNS-AS-RR(SHORT)	DNS-AS-RR(SHORT)			802.11e		
VoIP Telephony	app-class:VOIP-TELEPHONY	app-class:VO	business:yes	EF			Priority Queue (PQ)	Cisco IP Phones (G.711, G.729)
Broadcast Video	app-class:BROADCAST-VIDEO	app-class:BV	business:yes	CS5			(Optional) PQ	Cisco IP Video Surveillance / Cisco Enterprise TV
Real-Time Interactive	app-class:REALTIME-INTERACTIVE	app-class:RTI	business:yes	CS4			(Optional) PQ	Cisco TelePresence
Multimedia Conferencing	app-class:MULTIMEDIA-CONFERENCING	app-class:MMC	business:yes	AF4			BW Queue + DSCP WRED	Cisco Jabber, Cisco WebEx
Multimedia Streaming	app-class:MULTIMEDIA-STREAMING	app-class:MMS	business:yes	AF3			BW Queue + DSCP WRED	Cisco Digital Media System (VoDs)
Network Control	app-class:NETWORK-CONTROL	app-class:NC	business:yes	CS6			BW Queue	EIGRP, OSPF, BGP, ISIS, HSRP, IKE
Signaling	app-class:SIGNALING	app-class:CS	business:yes	CS3			BW Queue	SCCP, SIP, H.323
Ops / Admin / Mgmt	app-class:OPS-ADMIN-MGMT	app-class:OAM	business:yes	CS2			BW Queue	SNMP, SSH, Syslog
Transactional Data	app-class:TRANSACTIONAL-DATA	app-class:TD	business:yes	AF2			BW Queue + DSCP WRED	ERP Apps, CRM Apps, Database Apps
Bulk Data	app-class:BULK-DATA	app-class:BD	business:yes	AF1			BW Queue + DSCP WRED	E-mail, FTP, Backup Apps, Content Distribution
Best Effort	app-class:BEST-EFFORD	app-class:BE	business:default	DF	0		Default Queue + RED	Default Class
Scavenger	app-class:SCAVENGER	app-class:SCV	business:no	CS1	0		Min BW Queue (Deferential)	YouTube, Netflix, iTunes, BitTorrent, Xbox Live

Common AVC Library – Easy QoS Integration

```
class-map match-all VOICE
   match protocol attribute traffic-class voip-telephony
   match protocol attribute business-relevance business-relevant
class-map match-all BROADCAST-VIDEO
   match protocol attribute traffic-class broadcast-video
   match protocol attribute business-relevance business-relevant
class-map match-all INTERACTIVE-VIDEO
   match protocol attribute traffic-class real-time-interactive
   match protocol attribute business-relevance business-relevant
class-map match-all MULTIMEDIA-CONFERENCING
   match protocol attribute traffic-class multimedia-conferencing
   match protocol attribute business-relevance business-relevant
class-map match-all MULTIMEDIA-STREAMING
   match protocol attribute traffic-class multimedia-streaming
   match protocol attribute business-relevance business-relevan
 class-map match-all SIGNALING
   match protocol attribute traffic-class signaling
   match protocol attribute business-relevance b       s-relevant
class-map match-all NETWORK-CONTROL
   match protocol attribute traffic-class network-control
   match protocol attribute business-relevance business-relevant
class-map match-all NETWORK-MANAGEMENT
   match protocol attribute traffic-class ops-admin-mgmt
   match protocol attribute business-relevance business-relevant
class-map match-all TRANSACTIONAL-DATA
   match protocol attribute traffic-class transactional-data
   match protocol attribute business-relevance business-relevant
class-map match-all BULK-DATA
   match protocol attribute traffic-class bulk-data
   match protocol attribute business-relevance business-relevant
class-map match-all SCAVENGER
   match protocol attribute business-relevance business-irrelevant
```

"CISCO-CLS=app-name:WOLFGANG|app-class:NC"

magically allows "wolfgang.dns-as.org" to sneak underneath class-map NETWORK-CONTROL With ZERO configuration

```
policy-map MARKING
   class VOICE
     set dscp ef
   class BROADCAST-VIDEO
     set dscp cs5
   class INTERACTIVE-VIDEO
     set dscp cs4
   class MULTIMEDIA-CONFERENCING
     set dscp af41
   class MULTIMEDIA-STREAMING
     set dscp af31
   class SIGNALING
     set dscp cs3
   class NETWORK-CONTROL
     set dscp cs6
   class NETWORK-MANAGEMENT
     set dscp cs2
   class TRANSACTIONAL-DATA
     set dscp af21
   class BULK-DATA
     set dscp af11
   class SCAVENGER
     set dscp cs1
   class class-default
     set dscp default
```

```
DNS-AS Metadata:
www.dns-as.org          TXT "CISCO-CLS=app-name:HTTP|app-class:TD"
wolfgang.dns-as.org     TXT "CISCO-CLS=app-name:WOLFGANG|app-class:NC"
```

7. Demo

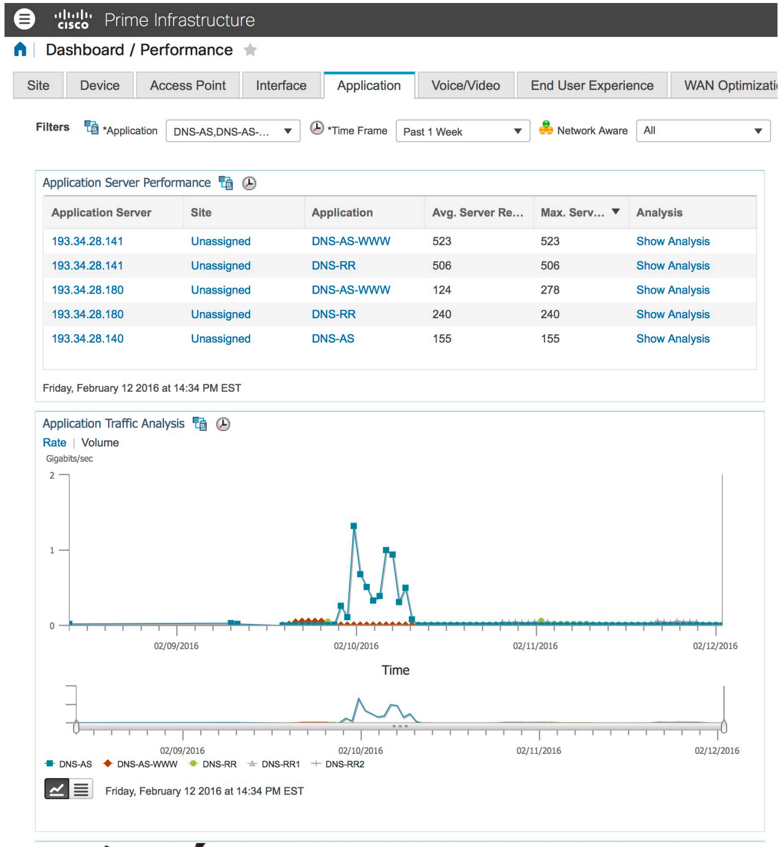
DNS-AS Visualization

DNS-AS Binding table into Prime Infrastructure and LiveAction

```
stealth-odd#show avc dns-as client binding-table

 ---------------------------------------------------------------------------------------------------------------------------------------------------------
 |                  |           |                |                         |      |                                                   |     | Time to |
 | Protocol name    | Vrf       | Ip List        | Host                    | Age  | Text record                                       | TTL | Expire  |
 |                  |           |                |                         |[min] |                                                   |[min]| [min]   |
 ---------------------------------------------------------------------------------------------------------------------------------------------------------
 | DNS-RR2          |<default>  |193.34.28.241   |rr2.f1-online.net        |4136  |app-name:DNS-RR2|app-class:NC|business:yes        |2879 |919      |
 | WWW0-PROXY2      |<default>  |193.34.28.245   |proxy2.f1-online.net     |4129  |app-name:WWW0-PROXY2|app-class:TD|business:yes    |2874 |<1       |
 | WWW0             |<default>  |193.34.29.161   |www.dns-as.org           |1767  |app-name:WWW0|app-class:TD                         |2879 |1112     |
 | DNS-RR1          |<default>  |193.34.29.241   |rr1.f1-online.net        |1235  |app-name:DNS-RR1|app-class:NC|business:yes        |2187 |950      |
 | N-BORDER         |<default>  |193.34.28.50    |border.dns-as.org        |733   |app-name:N-BORDER|app-class:TD|business:yes       |2879 |2145     |
 | N-CONNECT        |<default>  |193.34.29.50    |connect.dns-as.org       |511   |app-name:N-CONNECT|app-class:TD|business:yes      |2879 |2367     |
 ---------------------------------------------------------------------------------------------------------------------------------------------------------
```

```
stealth-even#show avc dns-as client binding-table
 ---------------------------------------------------------------------------------------------------------------------------------------------------------
 |                  |           |                |                         |      |                                                   |     | Time to |
 | Protocol name    | Vrf       | Ip List        | Host                    | Age  | Text record                                       | TTL | Expire  |
 |                  |           |                |                         |[min] |                                                   |[min]| [min]   |
 ---------------------------------------------------------------------------------------------------------------------------------------------------------
 | WWW0-PROXY2      |<default>  |193.34.28.245   |proxy2.f1-online.net     |4035  |app-name:WWW0-PROXY2|app-class:TD|business:yes    |1561 |<1       |
 | WWW0             |<default>  |193.34.28.47    |www.dns-as.org           |3560  |app-name:WWW0|app-class:TD|business:yes            |400  |37       |
 | VPN-GW-odd       |<default>  |193.34.31.242   |vpn-gw-odd.f1-online.net |3542  |app-name:VPN-GW-odd|app-class:BD|business:yes     |1297 |723      |
 | N-BORDER         |<default>  |193.34.28.153   |border.dns-as.org        |868   |app-name:N-BORDER|app-class:TD|business:yes       |802  |764      |
 | MX00             |<default>  |193.34.29.140,  |mail.dns-as.org          |430   |app-name:MX00|app-class:BD|business:yes            |2880 |2437     |
 |                  |           |193.34.28.140   |                         |      |                                                   |     |         |
 ---------------------------------------------------------------------------------------------------------------------------------------------------------
```

DNS-AS & PI Visualization per https app



Filters *Application DNS-AS,DNS-AS-... *Time Frame Past 1 Week Network Aware All

Application Server Performance

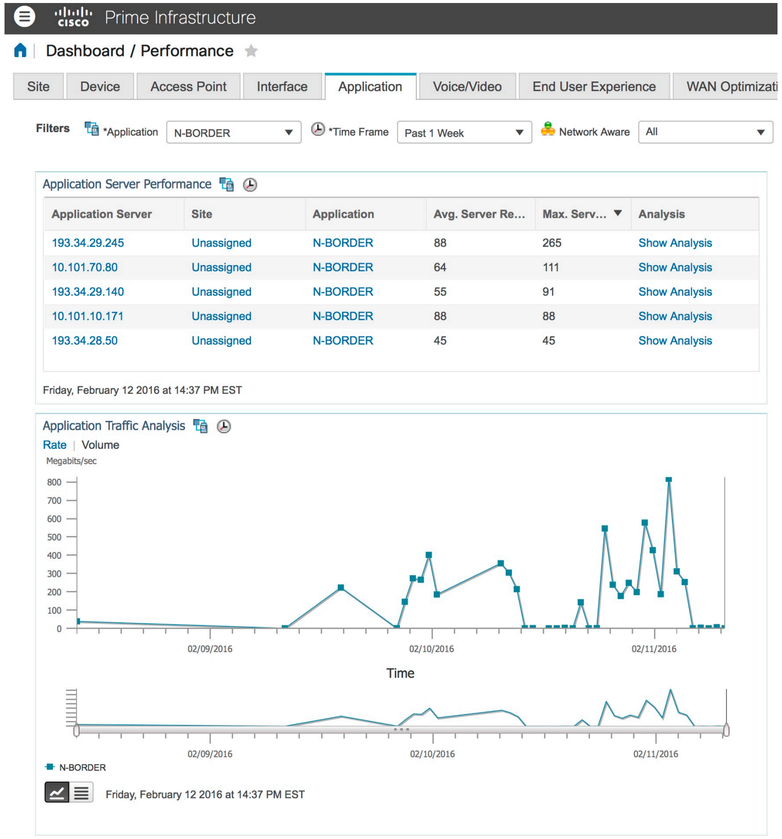
Application Server	Site	Application	Avg. Server Re...	Max. Serv...	Analysis
193.34.28.141	Unassigned	DNS-AS-WWW	523	523	Show Analysis
193.34.28.141	Unassigned	DNS-RR	506	506	Show Analysis
193.34.28.180	Unassigned	DNS-AS-WWW	124	278	Show Analysis
193.34.28.180	Unassigned	DNS-RR	240	240	Show Analysis
193.34.28.140	Unassigned	DNS-AS	155	155	Show Analysis

Friday, February 12 2016 at 14:34 PM EST

Application Traffic Analysis

Rate | Volume

Friday, February 12 2016 at 14:34 PM EST



Filters *Application N-BORDER *Time Frame Past 1 Week Network Aware All

Application Server Performance

Application Server	Site	Application	Avg. Server Re...	Max. Serv...	Analysis
193.34.29.245	Unassigned	N-BORDER	88	265	Show Analysis
10.101.70.80	Unassigned	N-BORDER	64	111	Show Analysis
193.34.29.140	Unassigned	N-BORDER	55	91	Show Analysis
10.101.10.171	Unassigned	N-BORDER	88	88	Show Analysis
193.34.28.50	Unassigned	N-BORDER	45	45	Show Analysis

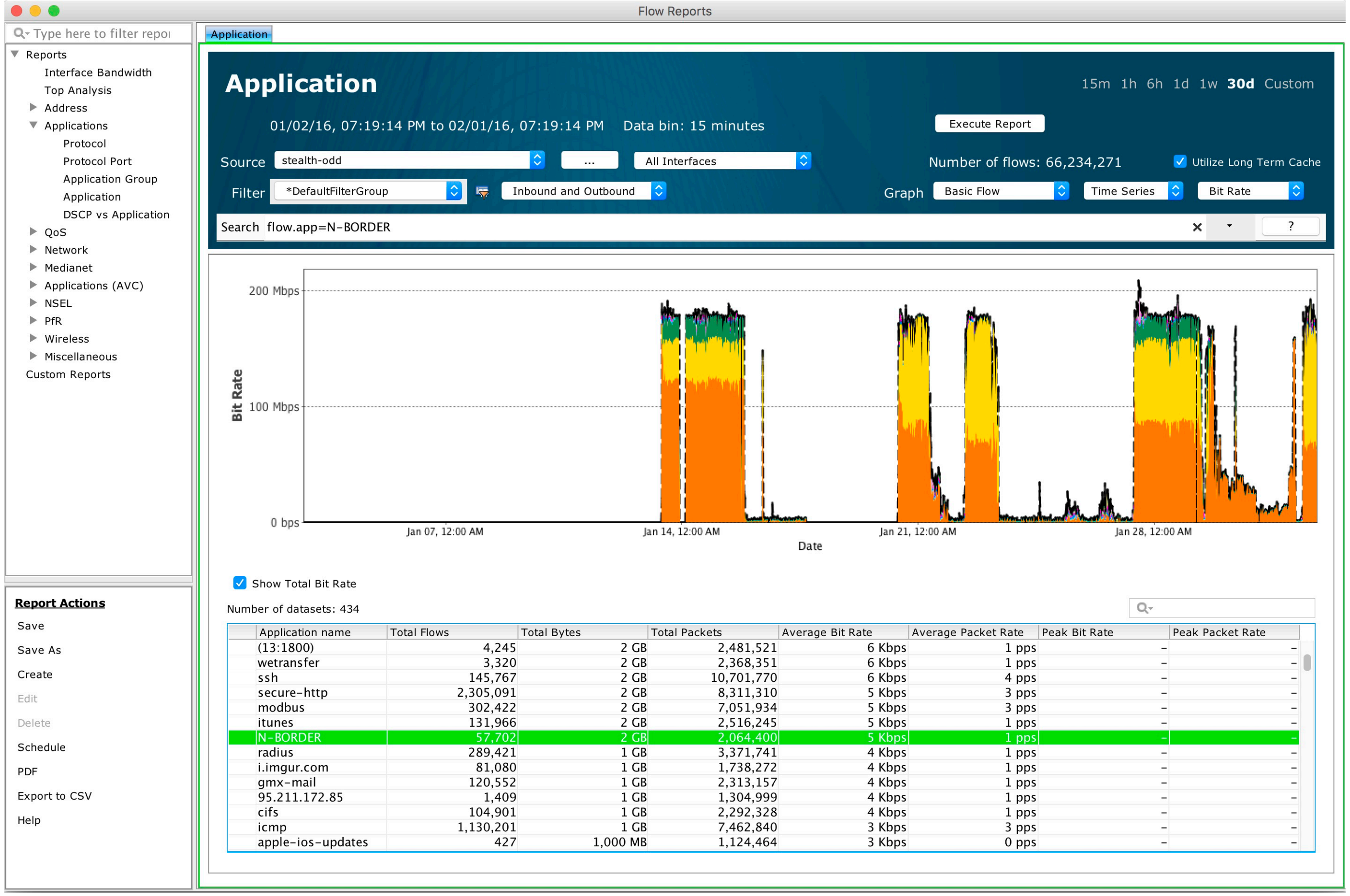
Friday, February 12 2016 at 14:37 PM EST

Application Traffic Analysis

Rate | Volume

Friday, February 12 2016 at 14:37 PM EST

DNS-AS & LiveAction Visualization per https app



Application

01/02/16, 07:19:14 PM to 02/01/16, 07:19:14 PM Data bin: 15 minutes

Source: stealth-odd | All Interfaces

Number of flows: 66,234,271

☑ Utilize Long Term Cache

Filter: *DefaultFilterGroup | Inbound and Outbound

Graph: Basic Flow | Time Series | Bit Rate

Search flow.app=N-BORDER

☑ Show Total Bit Rate

Number of datasets: 434

Application name	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
(13:1800)	4,245	2 GB	2,481,521	6 Kbps	1 pps	–	–
wetransfer	3,320	2 GB	2,368,351	6 Kbps	1 pps	–	–
ssh	145,767	2 GB	10,701,770	6 Kbps	4 pps	–	–
secure-http	2,305,091	2 GB	8,311,310	5 Kbps	3 pps	–	–
modbus	302,422	2 GB	7,051,934	5 Kbps	3 pps	–	–
itunes	131,966	2 GB	2,516,245	5 Kbps	1 pps	–	–
N-BORDER	57,702	2 GB	2,064,400	5 Kbps	1 pps	–	–
radius	289,421	1 GB	3,371,741	4 Kbps	1 pps	–	–
i.imgur.com	81,080	1 GB	1,738,272	4 Kbps	1 pps	–	–
gmx-mail	120,552	1 GB	2,313,157	4 Kbps	1 pps	–	–
95.211.172.85	1,409	1 GB	1,304,999	4 Kbps	1 pps	–	–
cifs	104,901	1 GB	2,292,328	4 Kbps	1 pps	–	–
icmp	1,130,201	1 GB	7,462,840	3 Kbps	3 pps	–	–
apple-ios-updates	427	1,000 MB	1,124,464	3 Kbps	0 pps	–	–

8. DNS-AS IOS CLI

IOS - Commands

CLI: Enable DNS-AS Client

- DNS-AS is disabled by default
- DNS-AS trusted-domain-filter is empty (whitelist model)
- DNS-AS is supported with both advance and standard images

```
1. conf t
2. avc dns-as client trusted-domains
3. domain <regular expression>
```

```
Example:

!
ip name-server vrf internet 193.34.29.241 193.34.28.241
ip domain round-robin
!
avc dns-as client enable
!
avc dns-as client trusted-domains
domain *.f1-online.net
domain *.toocoolforyou.net
domain *.dns-as.org
domain *.internal.cisco.com
domain ^.*cisco.*$
!
```

9. Program Plans & Milestones

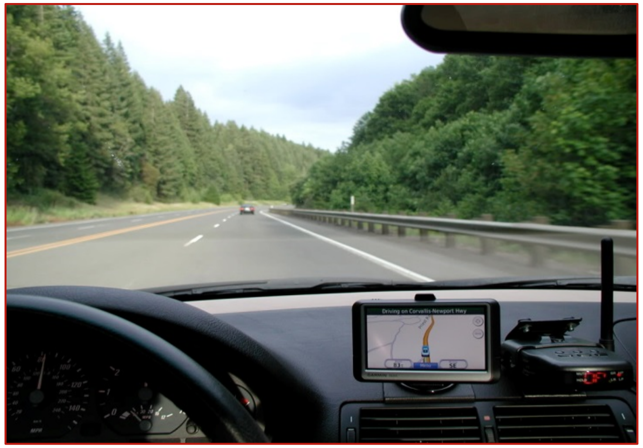
10. Conclusion and Open Discussion

We have come a Mile… but still a Way to Go!

Stages in the Application Assurance Lifecycle

Blindfolded ☹

Some Light…



Clear View ☺

Summary - Why DNS-AS ?

- Why would I want to make a best guess if I can know?
- As more CPU cycles you could free up by using DNS-AS as more you have left for running DPI
- DPI will have a hard time working with encrypted traffic
- DPI can never work at wire rate and as more throughput we need as less feasible DPI methods become
- Emerging protocols like SPDY, HTTP/2, QUIC makes it impossible to have a clear AVC view
- DPI as all other current methods just work if you have direct admin control over the box
- DNS-AS is single point of administration without the need for having admin control over the network's in between. As customers will have less and less own networks in the near future this is becoming more and more important to have a "controller" which doesn't imply having admin control over the ND itself.
- It's all about METADATA
- More info? Just visit www.ns-as.org

Lunch and Learn

LALCRS-0006 - APIC-EM - Thursday 18 February 13:00 – 14:15

During lunch on Tuesday, Wednesday and Thursday, you can join Cisco subject matter experts and your peers in these casual conversations about topics of interest to you.

The Lunch and Learn tables are located in the Catering Area in Hall 4.1.

For a full list of topics on each day, go to:

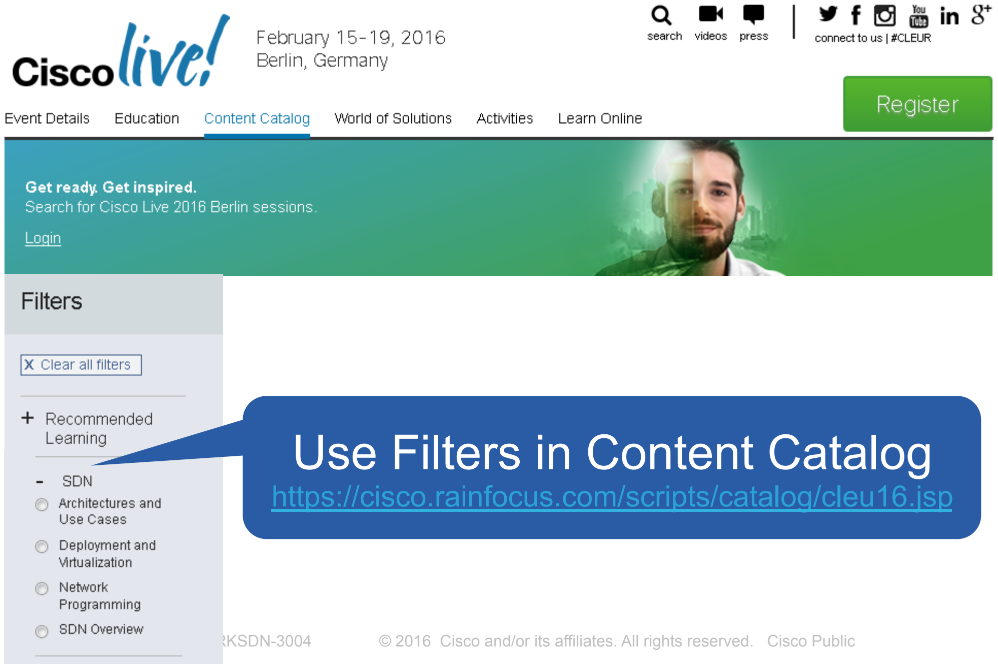
http://cs.co/berlin-lal

Cisco live!

SDN @ CiscoLive

- Recommended Learning Path on SDN
- 60+ Sessions
  - Technical Seminars
  - Breakout Sessions
  - Hands-on Labs
  - Panel Discussion
- DevNet Zone
- Demos, MTE, Lunch&Learn, Whisper Suites,and more ....

http://www.ciscolive.com/emea/



February 15-19, 2016
Berlin, Germany

Get ready. Get inspired.
Search for Cisco Live 2016 Berlin sessions.
Login

Filters

X Clear all filters

+ Recommended Learning

- SDN

○ Architectures and Use Cases

○ Deployment and Virtualization

○ Network Programming

○ SDN Overview

Use Filters in Content Catalog
https://cisco.rainfocus.com/scripts/catalog/cleu16.jsp

Enterprise SDN @ CiscoLive

Monday	Advanced APIC Enterprise Module: SDN Controller for the Campus and Branch - TECSDN-3600
Monday	Enterprise SDN: Architectures and Key Concepts - TECSDN-2602
Monday	Enterprise SDN: Advanced Network Programming - Hands-On Lab TECSDN-3602
Tuesday	APIC-EM: Controller Workflow and Use Cases - BRKARC-3004
Tuesday	IWAN management via APIC-EM (SDN Controller) - BRKSDN-2099
Tuesday	CCIE Skill Transformation to SDN Kungfu Master - BRKSDN-4005
Wednesday	SDN Enabled QoS-A Deep Dive - BRKSDN-2046
Wednesday	Hitchhiker's Guide to Device APIs - BRKSDN-1119
Wednesday	Containers on routers and switches: Run your apps and tools natively on Cisco boxes - BRKSDN-2116
Wednesday	Playing With Your Traffic: Exploring Software-Defined Packet Control - BRKSDN-3014
Wednesday	Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) – Hands on Lab - LTRSDN-1914
Thursday	APIC-EM: The evolution from traditional management to SDN-led, policy-based automation - BRKNMS-2031
Thursday	Cisco Open SDN Controller Hands-on Lab - LTRSDN-1913
Thursday	Deploying Cisco IOS Autonomic Networking Infrastructure - BRKSDN-2047
Thursday	DNS-AS: Done with SDN and Tired of Dealing with Snowflake Network Complexity? Change the Game with a Simple TXT String! - BRKSDN-3004
Friday	Solutions Enablement by Cisco Open SDN Controller - BRKSDN-1020

More SDN Sessions in the Recommended Learning Path

Thank you