Sales & Partner Training
Worldwide Sales Strategy & Operations

DNS-AS

Berényi Áron

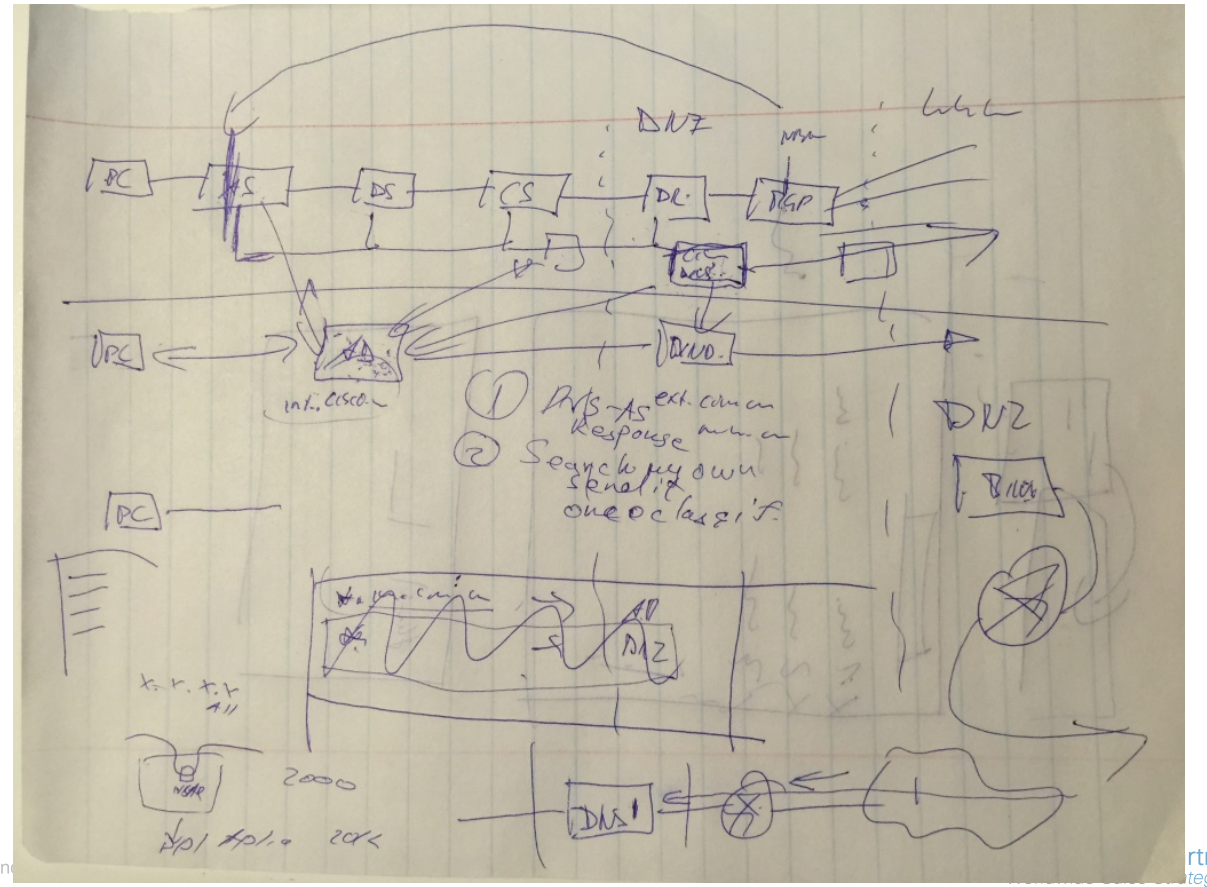
Cisco Systems

Introduction
What is DNS-AS ???

DNS-AS – The idea in 17.10.2013

Mike Herbert, Mark Montanez and Wolfgang Riedel @ a Sushi place in SJC

Sorry, no napkin this time…



DNS-AS - Tenets

Application Visibility

How

can you keep unambiguous visibility if the majority of traffic is encrypted?

Metadata Driven

How

can you holistically program the network so it behaves like a self driving car?

Centralized Control

How

to use DNS as a cross domain application intent policy controller?

How About DNS? – DNS server as a controller?

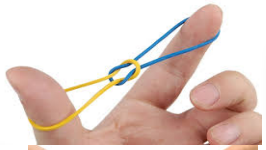
It's a pretty proven and awesome system, right?

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

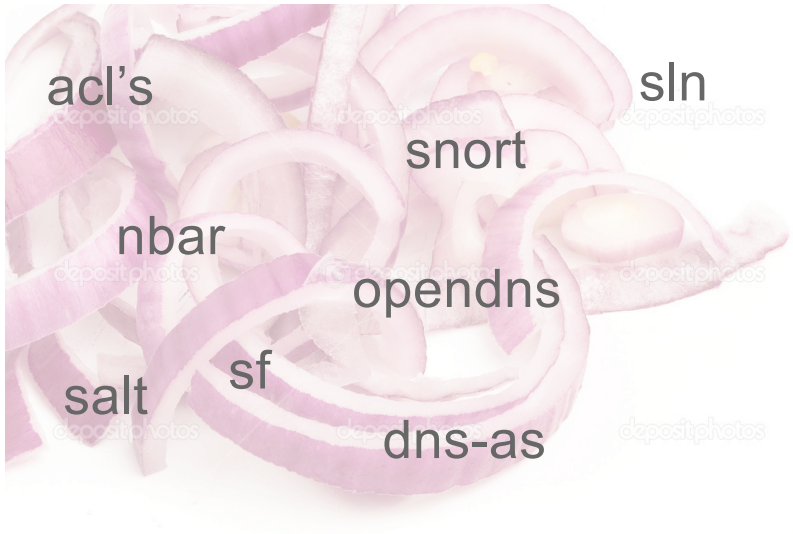
Has the capacity of Adaptive Evolution – Metadata not just limited to Network Devices

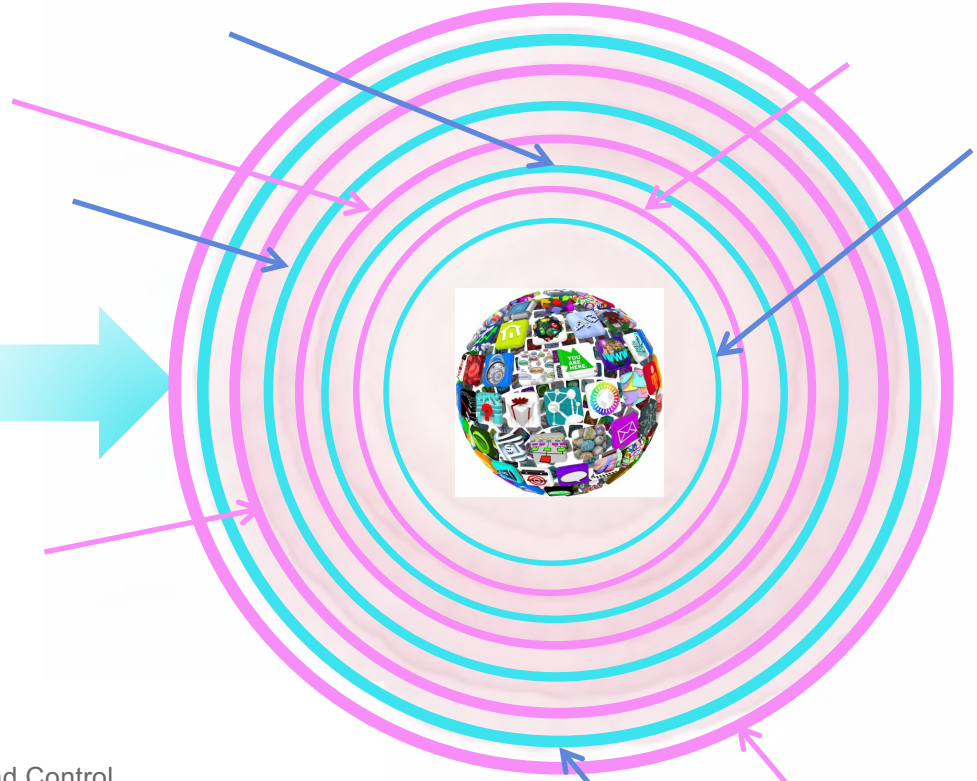
Performance

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

How About DNS-AS Integrations

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

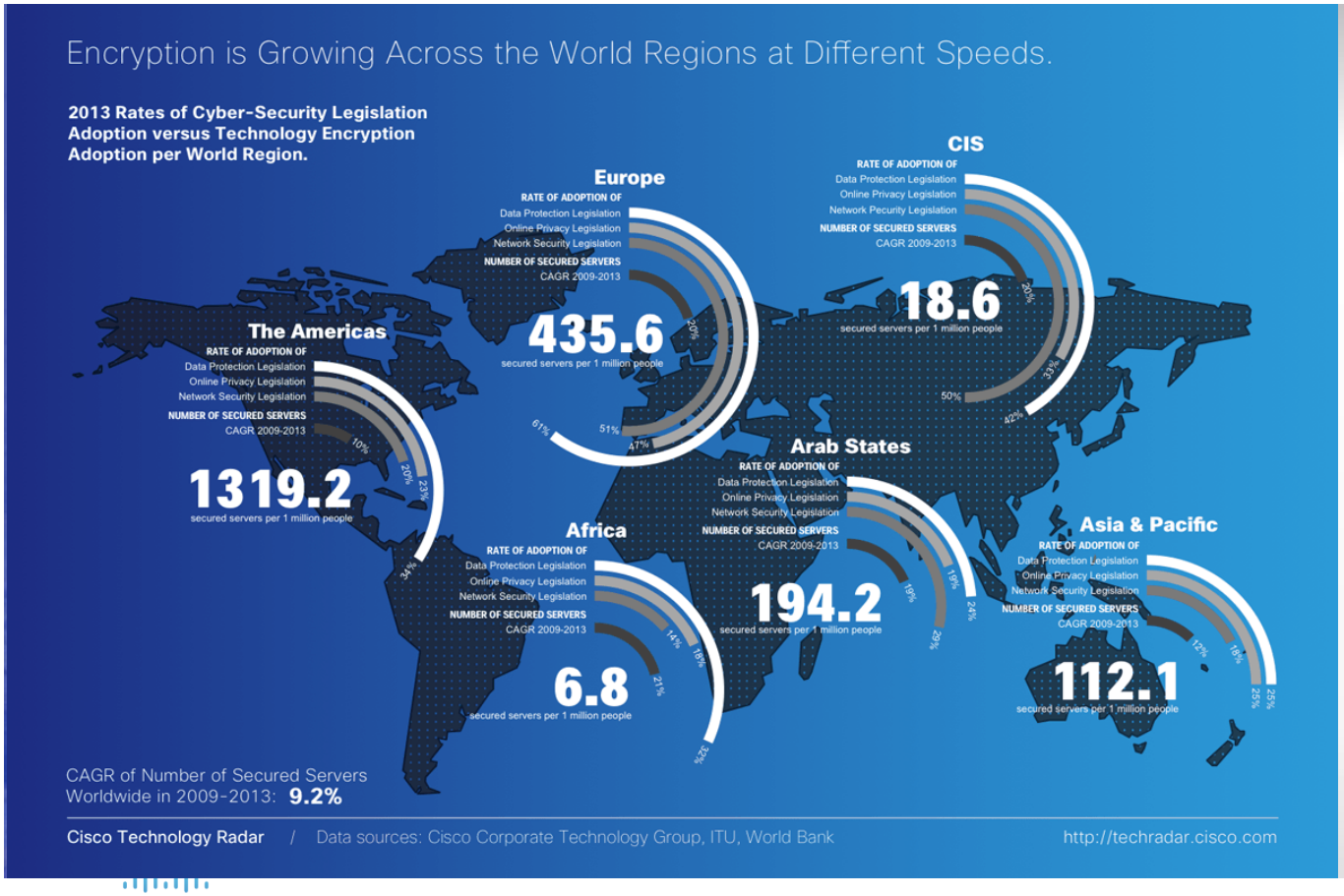
2. Principle: **Declarative Control**
Don't spend cycles trying to learn or guess what you can program

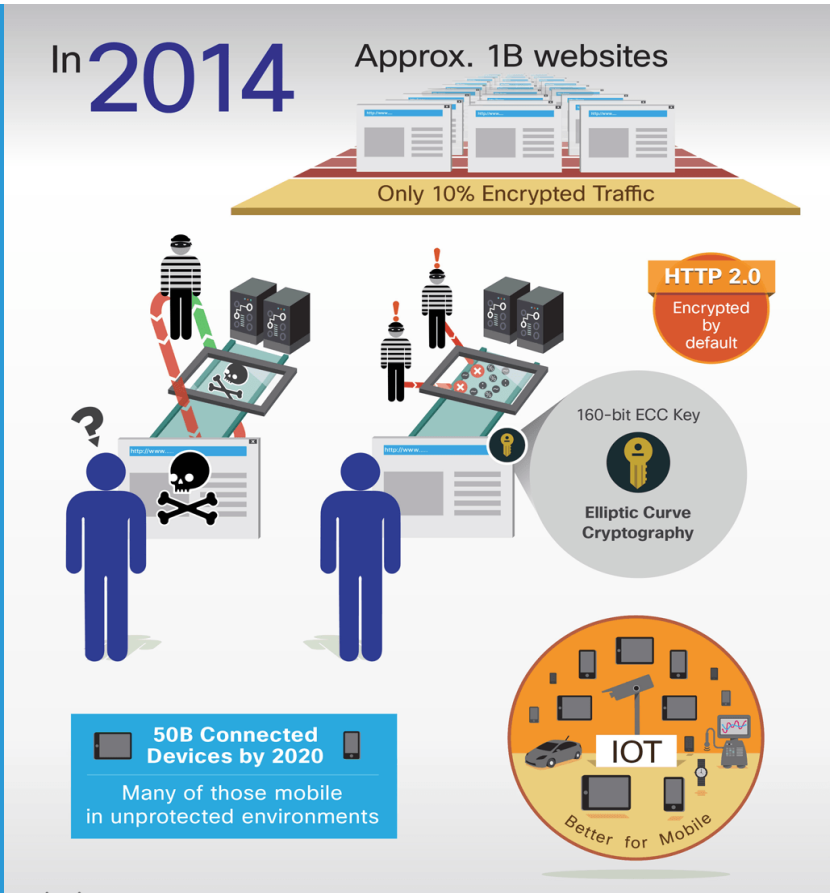
3. Principle: **Power of AND**
It's not about one is better then…
We need them all!

Application and Protocol challenges

The World Two Years After “Snowden”

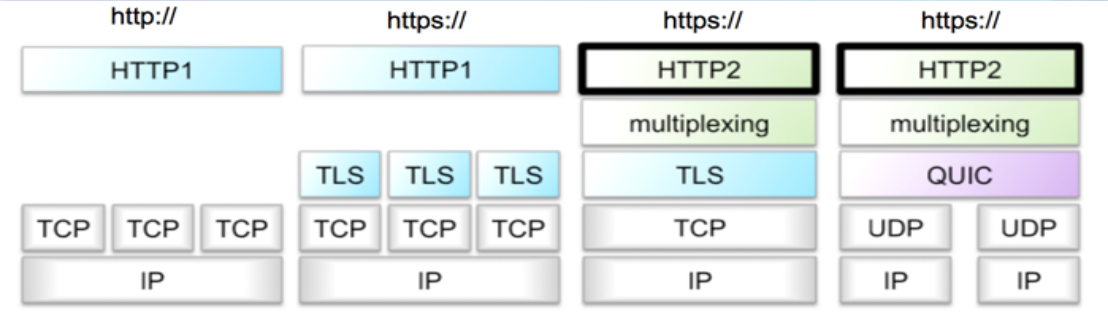
Growth of Encrypted Network Traffic

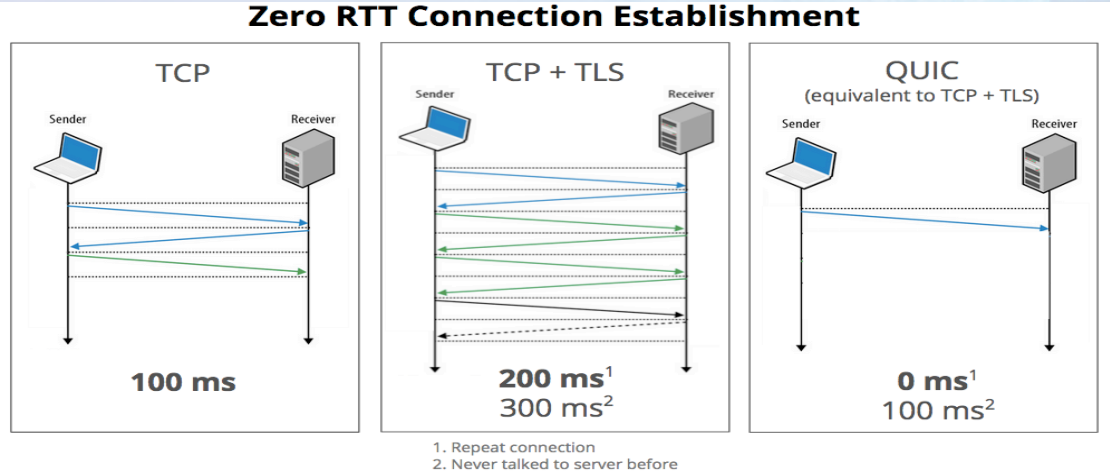




The World Two Years After “Snowden”

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





- HTTP/1.0 was pioneered in the late 80’s
- TCP + TLS requires 2 to 3 round trips
- HTTP/2 February 2015 IETF steering group announced completion
- Real performance improvement over TCP
- zero-round-trip connection establishment
- encryption capability by default
- SPDY: unlimited concurrent streams over a single TCP connection
- QUIC: bundles streams over the same UDP connection
- If your firewalls block bi-directional UDP traffic, QUIC is blocked also.
- How to differentiate your could delivered QUIC app from an UDP attack?
- How about ICMP to the host

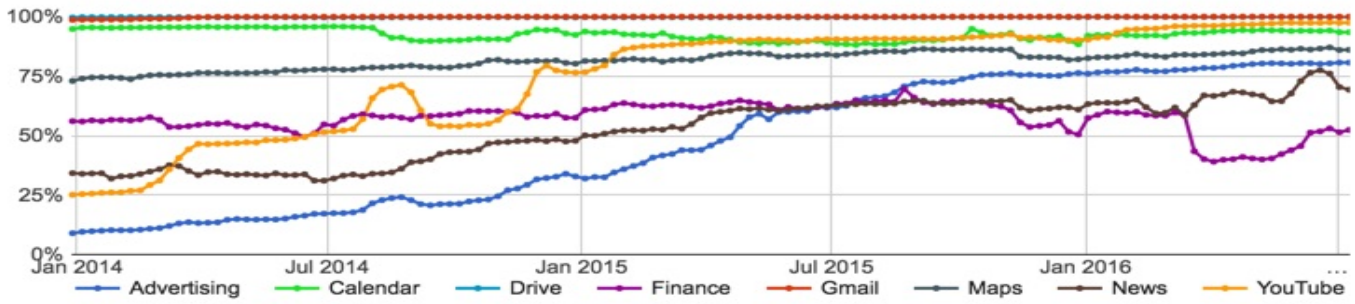
Living in a after “Snowden” world

Google Will Soon Shame All Websites That Are Unencrypted - Motherboard

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

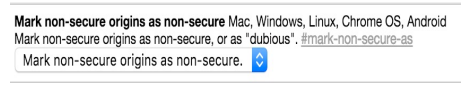
By Nathan Ingraham on November 21, 2013 02:50 pm Email @NateIngraham

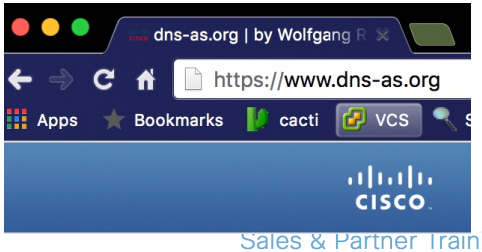
- Google wants everything on the web to be travelling over a secure channel.
- Google Announces 97 Percent of YouTube Traffic is Now Encrypted
- More important is to understand some implications:
  - Prevent content tampering, deny last mile SP to replace, add or filter out advertisement
  - Eliminating the ability of transparent proxies to muck up streaming protocols
  - Prevent last mile SP analytics, monitoring and monetization of user behavior
  - Net-Neutrality, Peering Agreements



This is an approximate number that represents most of Google traffic for the given product.

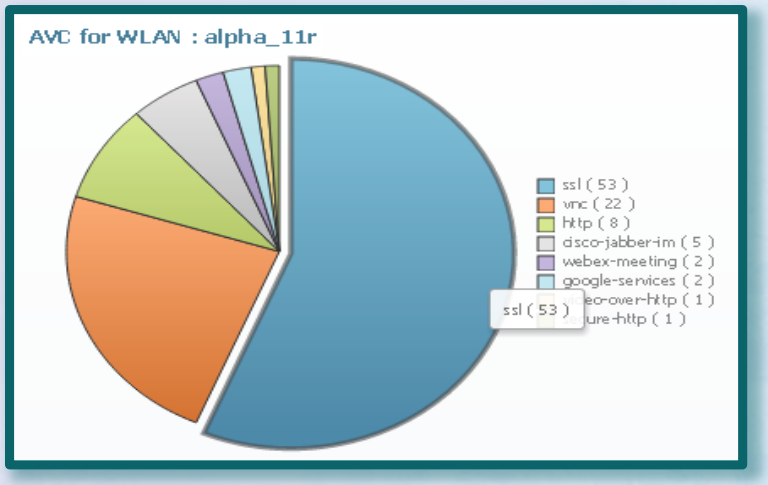
- Chrome: “chrome://flags”
- navigate to “mark non-secure as” and selecting “mark non-secure origins as non-secure.”





Living in a after “Snowden” world

It becomes harder and harder for us to “guess”



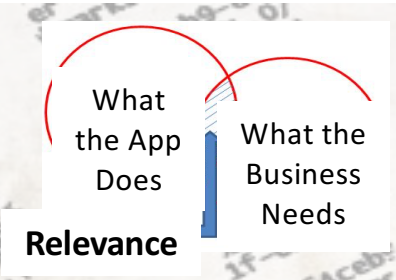
Bottom line: It becomes harder and harder for us to look into into traffic streams in order to “guess” what the apps are based on snooping traffic.

Network Metadata

Network Metadata

What is it? Why do we need it?

- literally, “data about the data”
  - Identify Enterprise Applications
  - Describe what the application **IS**
  - Describe what the application **NEEDS**
  - No longer any guessing



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

Application Network Metadata – DNS-AS

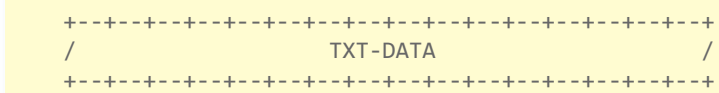
RFC6759 Metadata Components

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

DNS-AS Application Metadata – Where to store it?

RFC1035 Metadata Components within TXT and AVC RTYPEs

TXT RDATA format



TXT-DATA One or more <character-string>'s

- **depreciated** for DNS-AS
- to be used for backward compatibility reasons
- with not so current DNS servers
- before BIND 9.9.9b1

General DNS-AS TXT record syntax:
"CISCO-CLS=<option>:<val>{|<option>:<val>}*"

AVC RDATA format

AVC-DATA One or more <character-string>'s

- the official **IANA assigned** mnemonic
- preferred RR going forward if the authoritative DNS server already supports this new RR
- Starting with BIND 9.9.9b1 / BIND 9.10.4b2

General DNS-AS TXT record syntax:
"<option>:<val>{|<option>:<val>}*"

- You may have multiple "strings" in a single resource record
- Each "string" may be up to 255 characters in length
- RDATA itself may not exceed 65535 bytes in total
- That 64K limit is a general restriction on DNS records of all types
- Any DNS response which exceeds 512 bytes is slightly undesirable, or use EDNS0
- Responses which exceed 512 bytes will signal truncation and prompt a retry via TCP, optimal to stay within 512 bytes if possible.
- General DNS-AS RR record syntax: '<option>:<val>{|<option>:<val>}*'
- Option-value pairs may appear in the same record, separated by a pipe character '|'.
- Example for a TXT record with app metadata would be: **"CISCO-CLS=app-name:wolfgang|app-id:CU/67244"**
- Example for a AVC record with app metadata would be: **"app-name:wolfgang|app-id:CU/67244"**

DNS-AS Application Metadata – Mixed RDATA?

Metadata Lookup Sequencing with mixed TXT and AVC RTYPEs

Default RDATA Lookup Sequence:

```
1. query for AVC RDATA
        QTYPE=AVC for wolfgang.dns-as.org
        -> "app-name:dns-as-wolfgang|app-class:TD|business:YES|app-id:CU/28203”
        if NODATA or ANCOUNT=0 then goto 2

2. query for RPZ RDATA
        QTYPE=AVC for _avc.wolfgang.dns-as.org
        -> "app-name:dns-as-wolfgang|app-class:TD|business:YES|app-id:CU/28203”
        if NODATA or ANCOUNT=0 then goto 3

3. query for TXT RDATA
        QTYPE=TXT for wolfgang.dns-as.org
        -> "CISCO-CLS=app-name:dns-as-wolfgang|app-class:TD|business:YES|app-
        id:CU/28203”
        if NODATA or ANCOUNT=0 then goto 4

4. no DNS-AS related metadata available
           -> NBAR
```

Override options by trusted-domains:

```
!
avc dns-as client enable
!
avc dns-as client trusted-domains
 domain ^.*f1.*$ AVC RPZ TXT
 domain ^.*cisco.*$ TXT RPZ AVC
 domain *.toocoolforyou.net AVC RPZ TXT
 domain *.blackberry.net TXT
 domain *.dns-as.org AVC
 domain *.nbar2web.org
 domain *.f1-consult.com RPZ
 domain *.f1-consult.de
 domain *.f1-online.net
 domain *.f1v4.net
 domain *.f1v6.net
!
```

We need to accommodate:

- Zones that provide their own AVC information
- Zones who don't provide any AVC information
- Zones whose provided AVC information you want to override locally
- All other DNS lookups passing unimpeded/unaltered

- Query in that sequence and just sent the QTYPES been listed behind the trusted-domain label.
- If there is no QTYPE listed, just follow the default lookup sequence.

Network Metadata – AVC Components

Metadata Components for Application Visibility

Important Application Visibility Attributes:

- ✓ Application Name (app-name)
- ✓ Application ID (app-id)

Optional Application Visibility Attributes:

- Attributes (tunneled, encrypted, p2p)
- Server Port Range (to identify an application with ports)
- IP Protocol Specifier
- IP Version Specifier
- Source of Metadata (NBAR2, DNS-AS server etc.)

```
TXT Example:
"CISCO-CLS=app-name:smtp|app-id:IL4/25|server-port:TCP/25,UDP/25”
```

```
AVC Example:
"app-name:smtp|app-id:IL4/25|server-port:TCP/25,UDP/25”
```

Network Metadata – AVC Components

Metadata Components for Application Policy Intent

Important Application Intent Attributes:

- ✓ Traffic Class (app-class)
- ✓ Business Relevance (business)

Optional Application Intent Attributes:

- Application Category
- Application Sub-Category
- Server Port Range (to identify an application with ports)
- Min/Avg/Max Bandwidth consumption
- Max. Possible Packet Loss (in %)
- Max. Possible Jitter (in ms.)
- Max. Possible Latency (in ms.)

TXT Example:

```
"CISCO-CLS=app-name:smtp|app-class:bulk-data|business:YES|app-id:IL4/25|server-port:TCP/25,UDP/25”
```

AVC Example:

```
"app-name:smtp|app-class:bulk-data|business:YES|app-id:IL4/25|server-port:TCP/25,UDP/25”
```

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

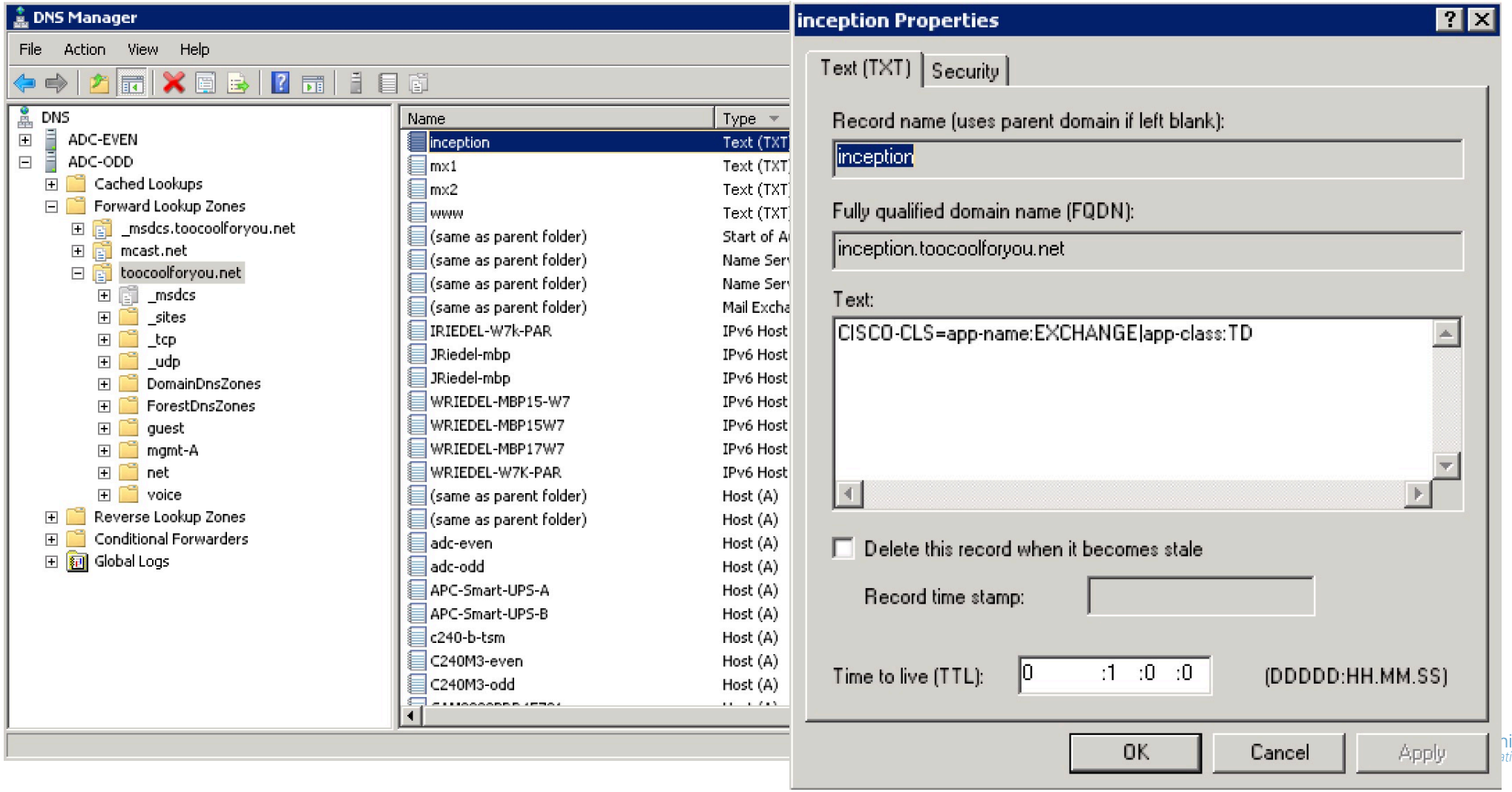
Forward Zone:

```
 [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 – Microsoft Active Directory



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 BIND	CLI, DLZ, SDB, Python, DynDB,	BIND 9

Source: Gartner (February 2015)

Network Metadata – Abstractions

Microsoft Office 365 with and without DNS-AS

without DNS-AS

*.outlook.com
*.microsoftonline.com
*.microsoftonline-p.com
*.microsoftonline-p.net
*.microsoftonlineimages.com
*.microsoftonlinesupport.net[1]
*.msecnd.net
*.office365.com
*.live.com
*.portal.microsoftonline.com
*.passwordreset.microsoftonline.com
*.msn.com
*.osub.microsoft.com

Ports 80/443
Protocols TCP and HTTPS
Rule must apply to all users
HTTPS/SSL time-out set to 8 hours

In reality, more then 120 entries

A full listing can be found here:
http://www.dns-as.org/support/das-as-cloud-apps/

with DNS-AS

DNS-AS metadata provided by MS:

```
AVC     "app-name:ms-update |app-class:BD|business=yes“
AVC     "app-name:ms-office365-web |app-class:BE|business=yes“
AVC     "app-name:ms-office365-outlook |app-class:BE|business=yes“
AVC     "app-name:ms-office365-live |app-class:MMS|business=yes"
AVC     "app-name:ms-office365-lync |app-class:VO|business=yes“
AVC     “ ... „
```

DNS-AS metadata consumed by customers

```
avc dns-as client trusted-domains
 domain ^.*outlook.*$
 domain ^.*microsoft.*$
 domain ^.*lync.*$
 domain ^.*sway.*$
```

DNS-AS Operations

DNS-AS-Client - Operations

DNS-AS Client (APs, Switches, Routers)

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

e A | 193.34.28.202
e TXT | "CISCO-CLS=app-name:HTTP|app-class:TD"

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

Authoritative DNS DNSSEC [external zones]

DNS Providers [forwarders] (OpenDNS, Google)

Recursive DNS [caching recursive resolvers] [RPZ slaves]

User

192.168.160.10

DNS-AS Client
192.168.254.100

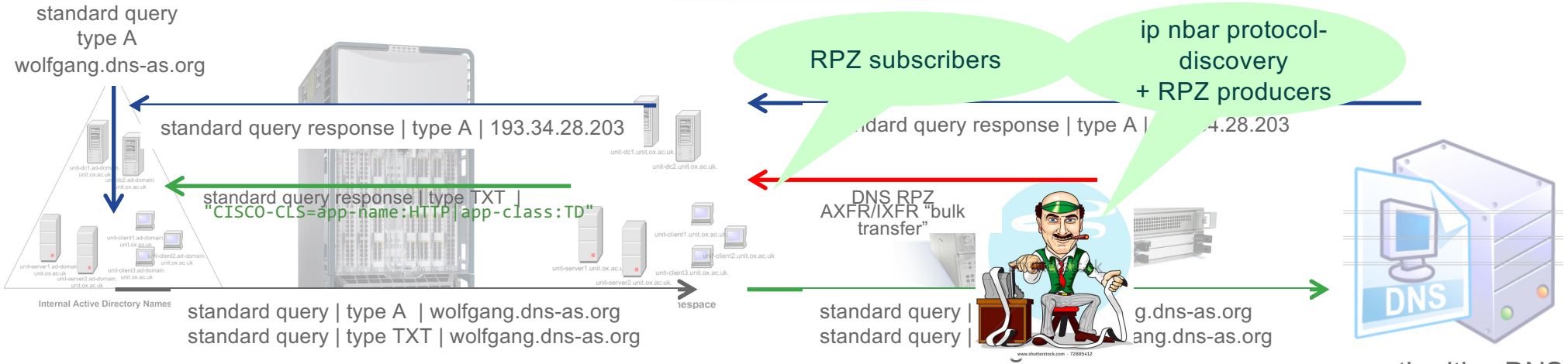
DNS snooping

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

standard query response | type A | 193.34.28.202

DNS-AS-Proxy - Operations

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



Actually, what can we do with it?

Common AVC Library – DNS-AS Use Case Matrix

DNS-AS <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
```

Easy QoS Integration

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

APPLICATION CLASS (RFC 4594)	APPLICATION CLASS long DNS-AS-RR (LONG)	APPLICATION CLASS short DNS-AS-RR(SHORT)	BUSINESS-RELEVANCE DNS-AS-RR(SHORT)	DSCP	COS	WMM 802.1 1e	QUEUING & DROPPING	APPLICATION EXAMPLES
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

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-interact
   match protocol attribute business-relevance business-r
class-map match-all MULTIMEDIA-CONFERENCING
   match protocol attribute traffic-class multimedia-c
   match protocol attribute business-relevance busine
class-map match-all MULTIMEDIA-STREAMING
   match protocol attribute traffic-class multimedia-s
   match protocol attribute business-relevance business
 class-map match-all SIGNALING
   match protocol attribute traffic-class signali
   match protocol attribute business-relevanc
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
     et dscp cs4
     MULTIMEDIA-CONFERENCING
     cp af41
     IMEDIA-STREAMING
     af31
     LING
     cs3
     ORK-CONTROL
     cp cs6
     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"
```

DNS-AS – Switches (no NBAR)

Catalyst 4k / Catalyst 2k

DNS-AS Classification & Marking Policy Example (Part 1 of 3)

```
!
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 REAL-TIME-INTERACTIVE
 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-relevant
class-map match-all SIGNALING
 match protocol attribute traffic-class signaling
 match protocol attribute business-relevance business-relevant
cla
 ma
 ma
cla
 ma
 ma
cla
 ma
 ma
cla
 ma
 match protocol attribute business-relevance business-relevant
class-map match-all SCAVENGER
 match protocol attribute business-relevance business-irrelevant
!
```

```
!
policy-map INGRESS-MARKING
 class-map match-all AUTOQOS_VOIP_VIDEO
  match cos  4
 class-map match-all AUTOQOS_VOIP_VOICE
  match cos  5
 class-map match-all AUTOQOS_VOIP_SIG
  match cos  3
!
```

Same ‘holy grail’ classification policy as on other router/switch platforms

Same ‘holy grail’ marking policy as on other router/switch platforms

Small extension of the trust boundary for voice and video

```
!
policy-map INGRESS-MARKING
 class VOICE
  set dscp ef
 class BROADCAST-VIDEO
  set dscp cs5
 class REAL-TIME-INTERACTIVE
  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
!
```

Catalyst 4k / Catalyst 2k

DNS-AS Classification & Marking Policy Example (Part 2 of 3)

```
!
interface GigabitEthernet2/14
 description IP-Phone
 switchport access vlan 165
 switchport mode access
 switchport voice vlan 111
 switchport port-security maximum 3
 switchport port-security violation restrict
 switchport port-security aging time 2
 switchport port-security aging type inactivit
 switchport port-security
 load-interval 30
 power inline police
 power efficient-ethernet auto
 auto qos voip cisco-phone
 storm-control broadcast level 10.00
 storm-control action trap
 qos trust device cisco-phone
 spanning-tree portfast edge
 spanning-tree bpduguard enable
 service-policy input INGRESS-MARKING
 service-policy output EGRESS-QUEUEING-1P7Q1T
!
```

In case trust boundary is extended to cisco-phone

Allow DSCP marking through the ingress policy-map

```
!
policy-map INGRESS-MARKING
 class AUTOQOS_VOIP_VOICE
  set dscp ef
  police cir 128000 bc 8000 conform-action
transmit  exceed-action set-dscp-transmit cs1
violate-action set-cos-transmit 1
 class AUTOQOS_VOIP_VIDEO
  set dscp af41
  police cir 10000000 bc 8000 conform-action
transmit  exceed-action set-dscp-transmit cs1
violate-action set-cos-transmit 1
 class AUTOQOS_VOIP_SIG
  set dscp cs3
  police cir 32000 bc 8000 conform-action
transmit  exceed-action set-dscp-transmit cs1
violate-action set-cos-transmit 1
!
```

Catalyst 4k / Catalyst 2k

DNS-AS Classification & Marking Policy Example (Part 3 of 3)

Configures basic DNS info

```
!
ip domain round-robin
ip domain-list toocoolforyou.net
ip domain-lookup source-interface Loopback0
ip domain-name toocoolforyou.net
ip name-server 192.168.167.244
ip name-server 192.168.168.244
!
```

DNS-AS snooping capability enabled by service-policy input

```
!
interface range TenGigabitEthernet2/1-40
 service-policy input INGRESS-MARKING
 service-policy output EGRESS-QUEUEING-1P7Q1T
!
```

Enables DNS-AS client

```
!
avc dns-as client enable
!
avc dns-as client trusted-domains
domain ^.*f1.*$
domain ^.*cisco.*$
domain *.toocoolforyou.net
domain *.dns-as.org
domain *.nbar2web.org
domain *.f1v4.net
domain *.f1v6.net
!
```

Whitelisted domains for which metadata may be queried and used for policy-purposes

DNS-AS – Routers (with NBAR)

ASR1k / ISR4k / CSR1kv

DNS-AS Classification & Marking Policy Example (Part 1 of 2)

```
!
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 REAL-TIME-INTERACTIVE
 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-relevant
class-map match-all SIGNALING
 match protocol attribute traffic-class signaling
 match protocol attribute business-relevance business-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
!
```

Same ‘holy grail’ classification policy as on other router/switch platforms

Same ‘holy grail’ marking policy as on other router/switch platforms

```
!
policy-map INGRESS-MARKING
 class VOICE
  set dscp ef
 class BROADCAST-VIDEO
  set dscp cs5
 class REAL-TIME-INTERACTIVE
  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
!
```

ASR1k / ISR4k / CSR1kv

DNS-AS Classification & Marking Policy Example (Part 2 of 2)

Configures basic DNS info

```
!
ip domain round-robin
ip domain-list toocoolforyou.net
ip domain-lookup source-interface Loopback0
ip domain-name toocoolforyou.net
ip name-server 192.168.167.244
ip name-server 192.168.168.244
!
```

DNS-AS snooping combined with NBAR

```
interface Giga  cEthernet0/0/0
 ip nbar protocol-discovery
 service-policy input ingress-MARKING
 service-policy output egress-hqos-95000
```

```
!
avc dns-as client enable
!
avc dns-as client trusted-domains
domain ^.*f1.*$
domain ^.*cisco.*$
domain *.toocoolforyou.net
domain *.dns-as.org
domain *.nbar2web.org
domain *.f1v4.net
domain *.f1v6.net
!
```

Enables DNS-AS client

Whitelisted domains for which metadata may be queried and used for policy-purposes

DNS-AS snooping without NBAR

```
interface Gigab  Ethernet0/0/0
 avc dns-as learning
 service-policy input ingress-MARKING
 service-policy output egress-hqos-95000
```

Program Plans & Milestones

DNS-AS Platform Plans & Milestones

Platform	Planned Release	Timeframe	Comments
Catalyst 2k 2960x, 2960xr, 2960cx	Danube	Jul 2016	DNS-AS Client (Basic)
Catalyst 3k 3560cx	Danube	Jul 2016	DNS-AS Client (Basic)
Catalyst 4k Sup7E, Sup8E & Sup8LE, 4500x	Danube	Jul 2016	DNS-AS Client (Basic)
Catalyst 6k	MK 4.1	CY 2017	N/A
Catalyst 3850 / 3650	Polaris 16.6	Sept 2016	DNS-AS Client (Basic)
ISRG2	N/A	N/A	N/A
ASR1k/ISR4k/CSR1kv	Polaris 16.2 – XE 3.18 GA	Mar 2016	DNS-AS Client (Basic)
NAM	TBD	TBD	TBD
WLC (AireOS)	TBD	TBD	TBD
IOS AP's	TBD	TBD	TBD
WLC (IOS)	Radar for Polaris 16.4	TBD	TBD
Nexus 5k, 6k, 7k	TBD	TBD	TBD

DNS-AS Visualization

DNS-AS Binding table into Prime Infrastructure and LiveAction

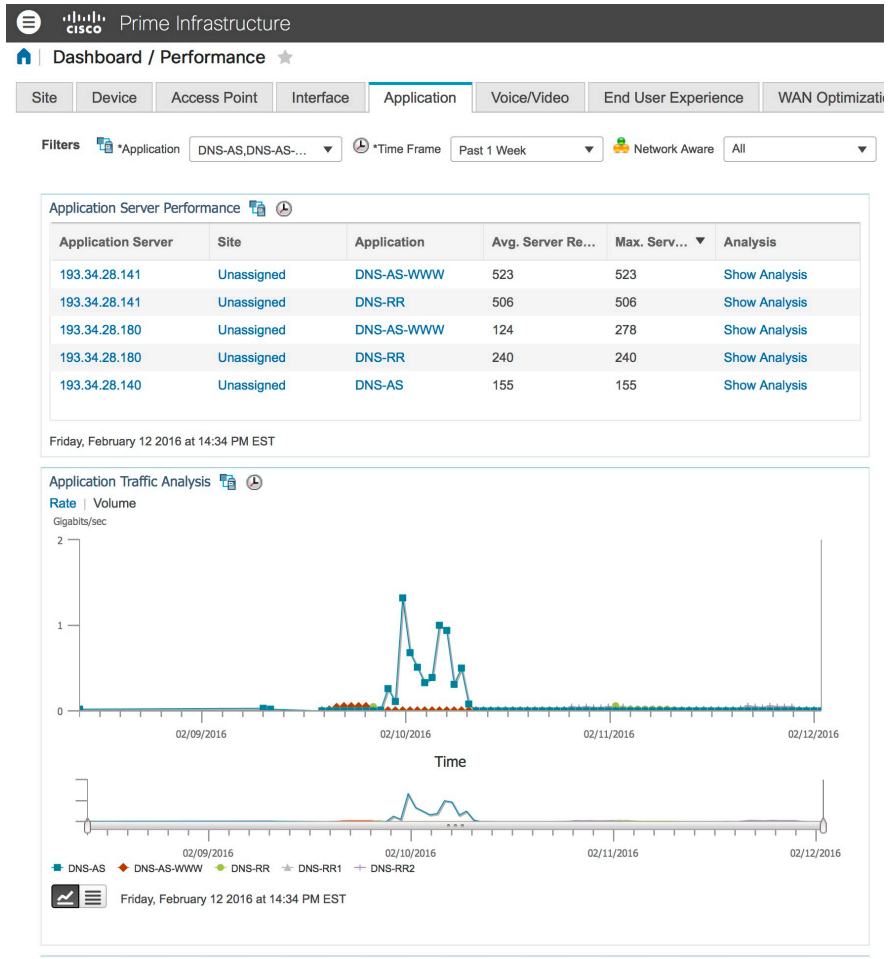
```
stealth-odd#show avc dns-as client binding-table
```

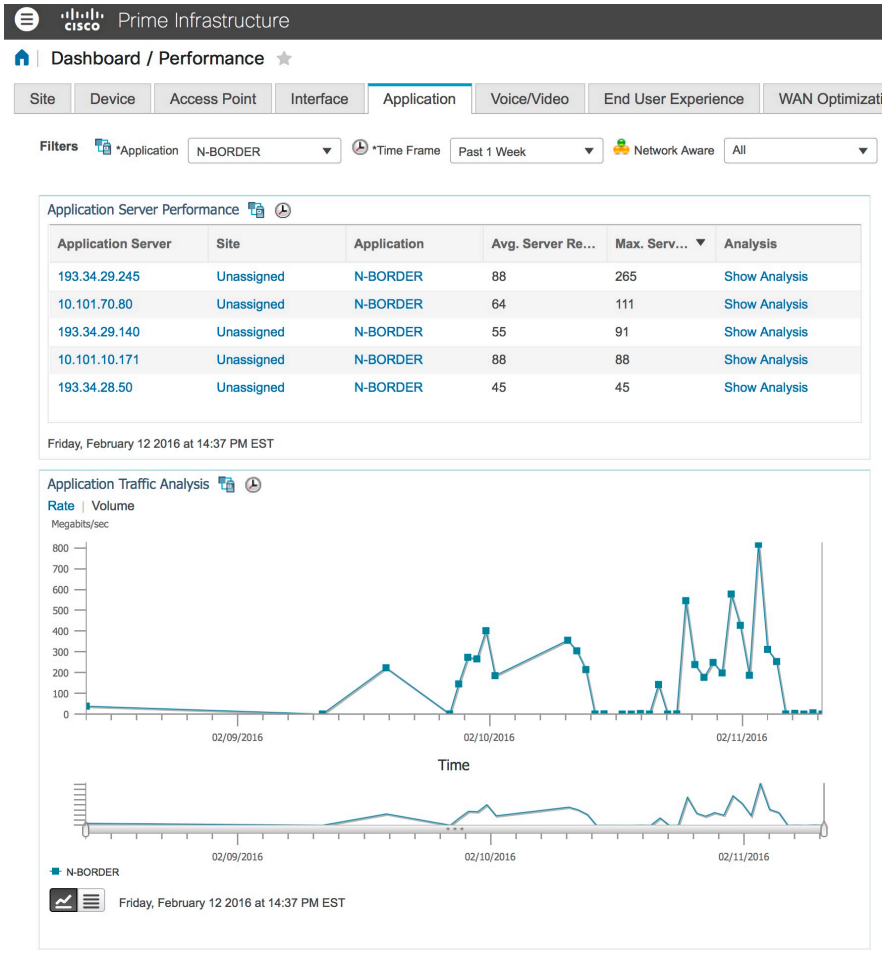
Protocol name	Vrf	Ip List	Host	Age [min]	Text record	TTL [min]	Time to Expire [min]
DNS-RR2	<default>	193.34.28.241	rr2.f1-online.net	4136	app-name:DNS-RR2|app-class:NC|business:yes	2879	919
WWW0-PROXY2	<default>	193.34.28.245	proxy2.f1-online.net	4129	app-name:WWW0-PROXY2|app-class:TD|business:yes	2874	<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
```

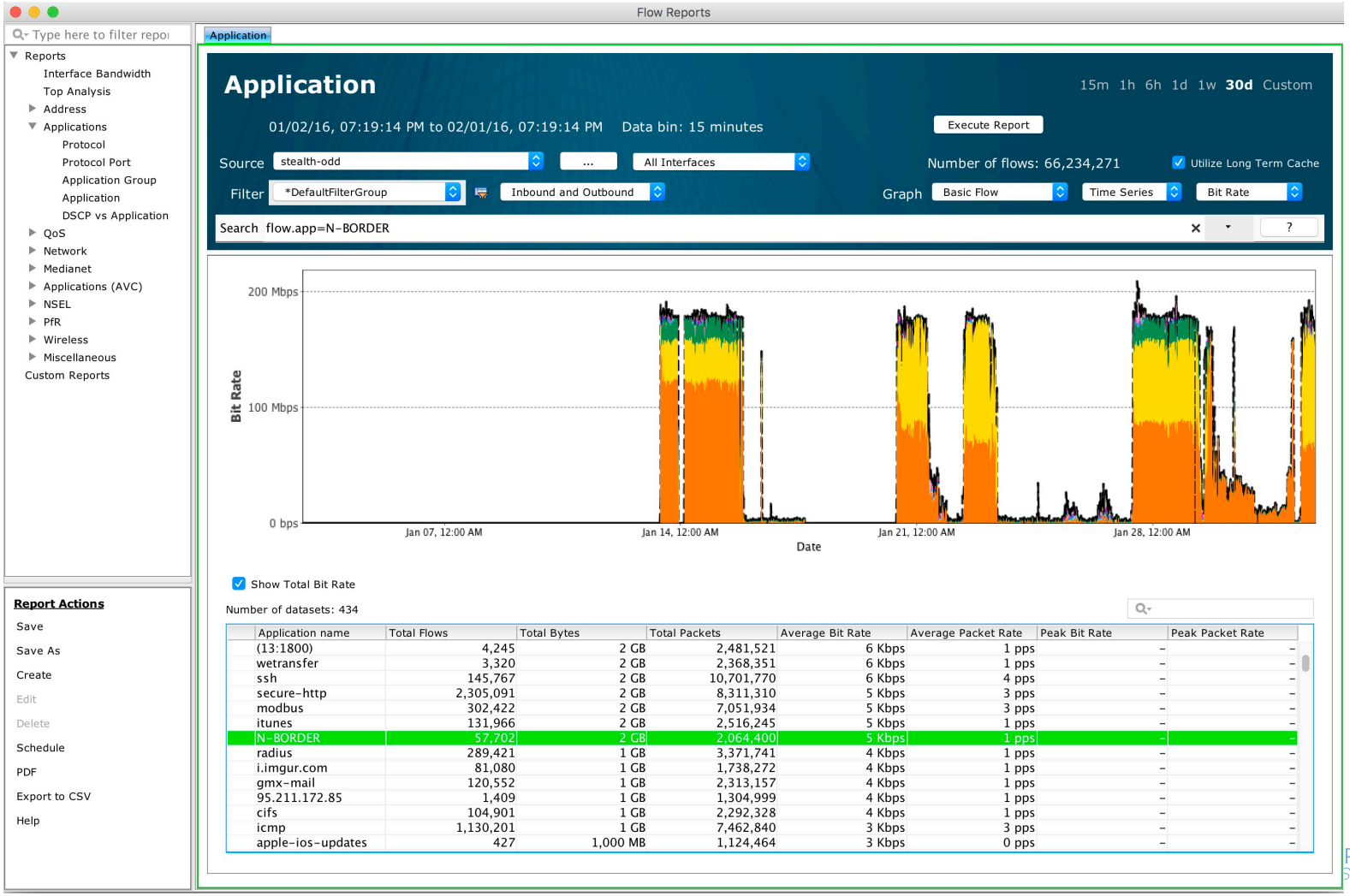
Protocol name	Vrf	Ip List	Host	Age [min]	Text record	TTL [min]	Time to Expire [min]
WWW0-PROXY2	<default>	193.34.28.245	proxy2.f1-online.net	4035	app-name:WWW0-PROXY2|app-class:TD|business:yes	1561	<1
WWW0	<default>	193.34.28.47	www.dns-as.org	3560	app-name:WWW0|app-class:TD|business:yes	400	37
VPN-GW-odd	<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, 193.34.28.140	mail.dns-as.org	430	app-name:MX00|app-class:BD|business:yes	2880	2437

DNS-AS & PI Visualization per https app





DNS-AS & LiveAction Visualization per https app



KÖSZÖNÖM A FIGYELMET

https://www.dns-as.org