OPS Area 综述及DNS相关工作

姚健康

2021.09 北京

IETF技术社群讨论

ops active WGs (15)

Group	Responsible AD	Name	Chairs
anima	Robert	Autonomic Networking Integrated Model and Approach	Toerless Eckert , Sheng Jiang
bmwg	Warren	Benchmarking Methodology	Sarah Banks , Al Morton
dime	Robert	Diameter Maintenance and Extensions	Jouni Korhonen , Lionel Morand
dnsop	Warren	Domain Name System Operations	Benno Overeinder , Tim Wicinski , Suzanne Woolf
grow	Warren	Global Routing Operations	Chris Morrow , Job Snijders
iotops	Warren	IOT Operations	Henk Birkholz , Alexey Melnikov
mboned	Warren	MBONE Deployment	Lenny Giuliano , Greg Shepherd
mops	Éric	Media OPerationS	Leslie Daigle , Kyle Rose (Assigned AD: Éric Vyncke)
netconf	Robert	Network Configuration	Mahesh Jethanandani , Kent Watsen
netmod	Robert	Network Modeling	Lou Berger , Joel Jaeggli , Kent Watsen
opsawg	Robert	Operations and Management Area Working Group	Henk Birkholz , Joe Clarke , Tianran Zhou
opsec	Warren	Operational Security Capabilities for IP Network Infrastructure	Ron Bonica , Jen Linkova
radext	Benjamin	RADIUS EXTensions	Lionel Morand , Stefan Winter (Assigned AD: Benjamin Kaduk)
sidrops	Warren	SIDR Operations	Chris Morrow , Keyur Patel
v6ops	Warren	IPv6 Operations	Fred Baker , Ron Bonica

思科谷歌 Operations and Management Area (ops)

Robert Wilton

Warren "Ace" K

- 解决协议在运行实施中的问题
- Operation
- Management

- **AD基本要全职工作**
- **大量阅读**
- **大量参与**
- **工作难度大**
- **能说能写（代码和文字）**

- OPS适合

✓一线运维经验

✓一线代码经验

✓开源代码维护者

Autonomic Networking Integrated Model and Approach (anima)

- 自主网络集成模型和方法（ANIMA）工作组开发和维护用于自动化网络管理和专业管理网络控制的互操作协议和程序的规范和文档。
- 工作范围：
  - ANI 的扩展
    - 包括 ANI 部署的变体（例如在虚拟化环境中）、AN 内的信息分发、ANI OAMP 接口（操作、管理、管理、供应）、与基于 YANG 的机制的交互、定义域边界和域的成员资格管理。
  - 支持自主服务代理，
    - 包括 ASA 的设计和实施指南、生命周期管理、ASA 的授权和协调。
  - BRSKI 功能，
    - 包括代理、注册、各种网络协议的适应、凭证格式的变化。

Autonomic Networking Integrated Model and Approach (anima)

- 工作范围：
  - 自主网络的通用用例及其新的GRAP扩展/选项
    - 包括批量传输、DNS-SD互通、自主资源管理、自主SLA保证、自主多租户管理、自主网络测量。
  - 与网络运营中心 (NOC) 的集成
    - 包括与 NOC 的自主发现/连接、NOC 基于 YANG 的 ANI/ASA 管理以及从节点向 NOC 报告 AF。
- Chairs
  - Sheng Jiang (华为技术有限公司网络技术实验室首席工程师)
  - Toerless Eckert (Futurewei Technologies Inc. USA)

Benchmarking Methodology (bmwg)

- 基准测试方法工作组（BMWG）将就互联网技术的关键性能特征或网络设备、系统和服务的基准提出一系列建议。
- BMWG的范围已扩展到开发虚拟网络功能（VNF）的方法以及配套的基础设施。
- 包括虚拟路由器、防火墙（和其他安全功能）、信令控制网关和其他形式网关的平台容量和性能特征基准。
- benchmarks将促进物理和虚拟网络功能之间的比较，并涵盖网络功能虚拟化系统的独特功能。此外，随着虚拟化测试系统的出现，测试系统校准规范也在范围之内。

Diameter Maintenance and Extensions (dime)

- Diameter协议是作为下一代的AAA协议标准,由RADIUS协议演进而来。Diameter（Radius的）维护和扩展工作组将重点关注Diameter协议的维护和扩展，以使其能够用于身份验证、授权、记帐、网络接入收费、网络内配置信息的提供，对于新的AAA会话管理，使用Diameter基本协议的扩展性规则。
- 工作范围：
  - 维护和/或推进Diameter基本协议和Diameter应用程序。包括对Diameter基本协议的扩展，可以将其视为功能增强或错误修复。
  - Diameter应用设计指南。将提供Diameter扩展的设计指南。详细说明何时考虑重用现有应用程序以及何时开发新应用程序。

Diameter Maintenance and Extensions (dime)

- 工作范围：
  - 用于批量和分组AAA会话管理的协议扩展。这项工作的目的是研究和标准化在Diameter基本协议上下文中处理AAA会话组的解决方案。该解决方案将定义如何在命令和操作中识别和处理分组AAA会话。
  - Diameter过载控制（overload control）。目的是确定当前Diameter基本协议提供的Diameter协议级别过载控制的局限性。将提供一套要求，以定义新的Diameter级别的过载控制机制。

Global Routing Operations (grow)

- 近年来，与BGP相关的操作问题的发生率有所增加，仍有很多问题需要解决，其中包括路由表增长率、内部和外部路由协议的交互、路由系统的动态特性以及路由策略对路由表的大小和动态性质的影响。此外，BGP的新的和创新的用途，例如将BGP用作某些类型的虚拟专用网络的信令协议，产生了新的和意想不到的操作问题。
- GROW工作组的目的是考虑与IPv4和IPv6全局路由系统相关的操作问题，包括但不限于路由表增长、内部路由协议和外部路由协议之间的交互作用以及地址分配策略和实践对全局路由系统的影响。
- GROW还将向包括IDR和RPSEC工作组在内的各工作组提供建议，说明其是否满足相关的操作需求，并在适当情况下提出修正建议。

Global Routing Operations (grow)

- 工作职责
  - Evaluate and develop various methodologies of controlling policy information in order to reduce the effect of prefix sub-aggregates beyond the necessary diameter, so as to reduce the Network Layer Reachability Information load on network infrastructure.
  - 记录当前部署的路由系统的问题并提出操作解决方案。
  - 分析支持新应用程序的各个方面需求，包括扩展现有路由协议和创建新路由协议。
  - 确定IGP扩展对Internet路由系统稳定性的影响。
  - Internet路由系统安全的操作方面。
- Chairs
  - Chris Morrow (Google)
  - Job Snijders (NTT Ltd.)

Global Routing Operations (grow)

已发布RFC（27篇 2005年 - 2019年）
RFC 8671 **Support for Adj-RIB-Out in the BGP Monitoring Protocol (BMP)**
RFC 8642 **Policy Behavior for Well-Known BGP Communities**
RFC 8327 **Mitigating the Negative Impact of Maintenance through BGP Session Culling**
RFC 8326 **Graceful BGP Session Shutdown**
RFC 8212 **Default External BGP (EBGP) Route Propagation Behavior without Policies**
RFC 8195 **Use of BGP Large Communities**
RFC 8050 **Multi-Threaded Routing Toolkit (MRT) Routing Information Export Format with BGP Additional Path Extensions**
RFC 7999 **BLACKHOLE Community**
RFC 7948 **Internet Exchange BGP Route Server Operations**
RFC 7908 **Problem Definition and Classification of BGP Route Leaks**
RFC 7789 **Impact of BGP Filtering on Inter-Domain Routing Policies**

Global Routing Operations (grow)

Active Internet-Drafts(4篇)
Support for Local RIB in BGP Monitoring Protocol (BMP)
AS Path Prepending
TLV support for BMP Route Monitoring and Peer Down Messages
Methods for Detection and Mitigation of BGP Route Leaks

IOT Operations (iotops)

- IotOps工作组专门讨论与物联网（IoT）设备相关的操作问题，物联网的定义比较模糊，就该工作组而言，其工作重点关注以下设备：
  - 已联网，无论是到 Internet 还是在有限的管理域内
  - 具有非常有限的最终用户界面或根本没有最终用户界面
  - 部署的数量足够多，无法轻松手动管理或维护
- Chairs
  - Alexey Melnikov (Isode Ltd)
  - Henk Birkholz (Fraunhofer SIT)

IOT Operations (iotops)

- 工作范围
  - 1) 参与并讨论与物联网设备操作管理相关的问题。这包括（但不限于）：
    - - 设备的工厂配置
    - - 设备入驻
    - - 设备对网络资源的访问控制
    - - 设备的管理控制
    - - 软件/固件升级
    - - 设备隔离
    - - 修复损坏的设备
    - - 设备的生命周期管理
  - 2) 听取意见并讨论与物联网运营安全相关的问题。
  - 3) 发布操作实践。

IOT Operations (iotops)

暂时没有已发布的RFC

Related Internet-Drafts (5 hits)
Secure IoT Bootstrapping: A Survey
A summary of security-enabling technologies for IoT devices
Different aspects of onboarding for IoT/Edge Devices
Involuntary Onwership Transfer of IoT devices: problem statement
A Taxonomy of operational security considerations for manufacturer installed keys and Trust Anchors

MBONE Deployment (mboned)

- MBONE部署工作组是协调全球互联网、域间和单域中组播路由协议的部署、工程化和操作的论坛。该活动将包括但不限于：
  - 全球互联网中组播路由的部署。
  - 接收有关多播技术部署的当前状态的定期报告。创建“实践和经验”文档，以获取已部署和正在部署各种组播技术的经验。
  - 根据报告和其他信息，向其他相关工作组提供反馈。
  - 开发共享操作信息的机制和程序，以帮助组播主干网和互连的操作。
  - 分析IPv4-IPv6组播过渡解决方案的需求。
  - 开发工具、扩展协议并提供操作和实施建议，以帮助在本机和非本机环境之间/内部进行组播管理、诊断、故障排除和部署。
- Chairs
  - Greg Shepherd (Cisco)
  - Lenny Giuliano (Juniper Networks)

Media OPerationS (mops)

- MOPS的工作重点是确定现有协议和/或网络在哪些领域将会受到新需求的挑战； MOPS 将就与媒体相关的运营问题和做法征求意见。
- 在本工作组范围内，媒体被视为包括视频、音频、对象及其任何组合的传输，可能是非顺序传输。
- 职责范围是媒体和媒体协议与网络的交互，而不是控制协议或媒体格式的技术。
- MOPS为视频行业和互联网工程专家提供了一个讨论视频技术对网络标准的要求的场所，以及在视频中IP技术新用途的建议。
- MOPS的目标包括记录互联网上媒体的现有协议和操作问题，以及确定潜在的IETF工作的需求。
- Chairs
  - Kyle Rose (Akamai Technologies, Inc.)
  - Leslie Daigle (ldaigle@thinkingcat.com)

Media OPerationS (mops)

- 工作职责
  - 从其他媒体技术开发联盟/标准机构处定期征求使用IETF开发协议的最新信息。
  - 征求网络运营商和用户的意见，以确定网络内和网络间媒体交付的问题，并确定这些问题的解决办法。
  - 就媒体获取和交付中的问题和机会，以及由此产生的协议和IETF之外开发的技术进行讨论。
  - 记录媒体采集（例如，从摄像机和记录设备）和交付的操作要求。
  - 开发操作运营信息，以帮助全球互联网媒体技术的运营管理。

Network Configuration (netconf)

- NETCONF 工作组，以前以 NETCONF 协议命名，现在更名为 NETwork CONFiguration 工作组。
- 负责YANG数据模型驱动管理的NETCONF、RESTCONF等协议的开发和维护。包括它们的传输和编码，定义支持协议所必需的数据模型，并定义支持使用协议的系统的操作部署的机制。
- NETCONF 协议是独立于数据建模语言的，但 YANG (RFC 7950) 是推荐的 NETCONF 数据建模语言，它引入了用于配置管理的高级语言功能。
- Chairs
  - Kent Watsen (Watsen Networks)
  - Mahesh Jethanandani (Kloud Services)

Network Configuration (netconf)

- 工作职责：
  - 网络管理协议NETCONF（rfc6241）。这项工作需要定期更新NETCONF相关规范，以满足新需求。
  - 网络管理协议 RESTCONF (RFC 8040)。这项工作需要定期更新 RESTCONF 相关规范，以应对出现的新需求。
  - 数据模型驱动协议使用的传输和编码。
  - 与网络管理协议相关的数据模型和机制。
  - 用于订阅数据的数据模型，以及用于将订阅的数据推送到客户端的协议绑定，以便进行监视和遥测。
  - 实现设备零接触设置和相关回拨功能的机制。

Network Modeling (netmod)

- 网络建模（NETMOD）工作组负责YANG数据建模语言，该语言可用于指定通过NETCONF和RESTCONF等协议传输的网络管理数据模型。
- NETMOD工作组讨论与YANG语言和YANG模型使用相关的主题，例如，将YANG模型数据映射到各种编码中。
- Chairs
  - Joel Jaeggli (Fastly)
  - Kent Watsen (Watsen Networks)
  - Lou Berger (LabN Consulting, L.L.C.)

Network Modeling (netmod)

- 工作职责
  - 维护数据建模语言YANG。这项工作需要定期更新规范，以满足出现的新需求。
  - 维护开发YANG模型的指导原则。这项工作主要是由YANG规范的更新驱动的。
  - 维护使用YANG模型的概念框架。这项工作需要描述YANG中存在的通用语境上下文，以及某些YANG语句在该语境中如何相互作用。 YANG与数据存储的关系就是一个例子。
  - 维护 YANG 建模数据的编码。这项工作需要更新NETMOD工作组已经定义的编码（XML和JSON），以适应YANG规范的变化，并定义所需的新YANG编码。
  - 维护用作基本YANG构建块的YANG模型。这项工作需要根据需要更新现有的YANG模型（ ietf-yang-types和ietf-inet-types ），并在必要时定义额外的核心YANG数据模型。
  - 定义和维护不属于任何其他现行IETF工作组章程范围内的YANG模型。

Operations and Management Area Working Group (opsawg)

- 运营和管理领域偶尔会收到关于发布涉及运营和管理主题的RFC的建议，**这些议题不在现有工作组的范围内，也没有理由成立新的工作组**。 OPSAWG将作为制定IETF中此类工作项目的论坛。
- 工作的重点将是规范O&M领域的行为。
- Chairs
  - Henk Birkholz (Fraunhofer SIT)
  - Joe Clarke (Cisco Systems, Inc.)
  - Tianran Zhou (Huawei)

Operations and Management Area Working Group (opsawg)

- 工作职责
  - O&M领域文档的模板和工具
  - 在已结束的工作组中开发的文件的维护和小规模扩展（例如MIB模块）。
  - RFC 5066“Ethernet in the First Mile Copper (EFMCu) Interfaces MIB”已转换为IEEE 802.3。然而，根据IEEE的协议，IF-CAP-STACK-MIB MIB模块（来自RFC5066）本质上是通用的，应继续得到IETF的支持。工作组将开发一份从RFC5066中提取IF-CAP-STACK-MIB的文件，强调该模块的通用性，并废止RFC5066。
  - 记录转换到 IEEE 802.3.1-2011 的 RFC 列表。考虑到RFC4663（将 MIB 工作从 IETF Bridge MIB WG 转移到 IEEE 802.1 WG ），将关注以下内容：旧IETF MIB名称与相应的新IEEE名称的映射表， IETF-IEEE交互的澄清/规则，及关于知识产权方面的澄清等。

Operational Security Capabilities for IP Network Infrastructure (opsec)

- OPSEC工作组将记录网络安全方面的操作问题和当前最佳实践。
- 工作职责
  - 对于讨论的每个主题，工作组将编制相应文件，其中包含与网络安全操作相关的常见做法。包括以下内容：
    - 要解决的一个或多个威胁
    - 应对威胁的现行做法
    - 编写本报告时存在的用于应对威胁的协议、工具和技术
    - 现有工具或技术中不存在解决方案的可能性
  - 这些文件会描述特定操作安全挑战或问题空间的范围，但不一定得出结论或提出解决方案
- Chairs
  - Jen Linkova (Google)
  - Ron Bonica (Juniper Networks)

RADIUS EXTensions (radext)

- RADIUS扩展工作组将重点关注对RADIUS（远程用户拨号认证系统）协议的扩展，并澄清其用法和定义。
- 此外，为了确保与现有RADIUS实现的向后兼容性，以及RADIUS和Diameter之间的兼容性，RADEXT WG考虑的扩展受到以下限制：
  - 生成的所有文档必须指定与旧RADIUS的互操作方式，如果可能，还必须与现有RADIUS RFC向后兼容。
- Chairs
  - Lionel Morand (Orange Labs)
  - Stefan Winter (RESTENA)

RADIUS EXTensions (radext)

- RADIUS扩展工作组近期目标：
  - CoA代理
    - 此工作项将描述如何在漫游环境中使用Operator-Name属性来代理CoA数据包，以确保只有授权代理才能将这些数据包发送到家庭CoA服务器。
  - 基于RADIUS的EAP响应/标识数据包的编码规则
  - 数据类型
    - 此工作项将定义数据类型，并更新IANA RADIUS属性类型注册表，以便每个属性都有一个数据类型
  - 更大的数据包
    - 使用此功能，通过RADIUS传输支持大于4096个八位字节的RADIUS数据包。
  - 用于IP端口配置和报告的RADIUS属性

SIDR Operations (sidrops)

- SIDR的全球部署（包括RPKI、BGP公告来源验证和BGPSEC）正在进行中，创建一个由SIDR感知和非SIDR感知网络组成的互联网路由系统。必须正确处理此部署，以避免将Internet划分为单独的网络。 Sidrops负责鼓励IDR技术的部署，同时确保在过渡期间全球路由系统尽可能安全。
- SIDR运行工作组（sidrops）为SIDR感知网络的运行制定指导方针，并就如何在现有和新网络中部署和运行SIDR技术提供运行指导。
- Chairs
  - Chris Morrow (Google)
  - Keyur Patel (Arrcus, Inc.)

SIDR Operations (sidrops)

- sidrops工作组的目标：
  - 征求一系列运营商的意见，以识别具有SIDR感知的互联网的操作问题，并确定这些问题的解决方案或变通办法。
  - 征求运营商的意见，以确定与不了解SIDR的互联网交互的问题，并确定这些问题的解决方案。
  - 为sidrops中确定的问题制定操作解决方案，并将其记录在BCP文件中。
  - IDR工作组主要负责域间路由协议的SIDR操作和部署问题以及BGPSEC维护和扩展。sidrops工作组可根据需要向该工作组提供投入，并与该工作组合作审查SIDR运行和部署问题的解决方案。

SIDR Operations (sidrops)

已发布RFC（8篇）
RFC 8481 **Clarifications to BGP Origin Validation Based on Resource Public Key Infrastructure (RPKI)**
RFC 8488 **RIPE NCC's Implementation of Resource Public Key Infrastructure (RPKI) Certificate Tree Validation**
RFC 8608 **BGPsec Algorithms, Key Formats, and Signature Formats**
RFC 8630 **Resource Public Key Infrastructure (RPKI) Trust Anchor Locator**
RFC 8634 **BGPsec Router Certificate Rollover**
RFC 8635 **Router Keying for BGPsec**
RFC 8893 **Resource Public Key Infrastructure (RPKI) Origin Validation for BGP Export**
RFC 8897 **Requirements for Resource Public Key Infrastructure (RPKI) Relying Parties**

IPv6 Operations (v6ops)

- IPv6的全球部署正在进行中，必须正确处理此部署，以避免将Internet划分为单独的IPv4和IPv6网络，从而确保所有IPv4和IPv6节点的寻址和连接。
- v6ops工作组为新的和现有的IPv6网络的部署制定操作指南。

- Chairs
  - Fred Baker (Formerly of Cisco, currently consulting)
  - Ron Bonica (Juniper Networks)

IPv6 Operations (v6ops)

- 工作组目标：
  - 征求网络运营商和用户的意见，以确定IPv6网络的部署问题，并确定这些问题的解决方案。
  - 征求网络运营商和用户的意见，以确定与IPv4网络的操作交互问题，并确定这些问题的解决方案。
  - 记录IPv6网络的操作要求。
  - 这些文档应记录IPv6运行经验，包括在双栈网络中与IPv4的交互、以IPv4作为覆盖（overlay）或转换服务的IPv6网络，或仅IPv6网络。

IPv6 Operations (v6ops)

已发布的RFC（81篇）
RFC 9098 Operational Implications of IPv6 Packets with Extension Headers
RFC 9096 Improving the Reaction of Customer Edge Routers to IPv6 Renumbering Events
RFC 8978 Reaction of IPv6 Stateless Address Autoconfiguration (SLAAC) to Flash-Renumbering Events
RFC 8683 Additional Deployment Guidelines for NAT64/464XLAT in Operator and Enterprise Networks
RFC 8585 Requirements for IPv6 Customer Edge Routers to Support IPv4-as-a-Service
RFC 8475 Using Conditional Router Advertisements for Enterprise Multihoming
RFC 8305 Happy Eyeballs Version 2: Better Connectivity Using Concurrency
RFC 8273 Unique IPv6 Prefix per Host
RFC 8215 Local-Use IPv4/IPv6 Translation Prefix
RFC 7934 Host Address Availability Recommendations
RFC 7872 Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World

IPv6 Operations (v6ops)

Active Internet-Drafts (2 hits)
IPv6 Deployment Status
Pros and Cons of IPv6 Transition Technologies for IPv4aaS

Domain Name System Operations (dnsop)

- dnsop工作组将为DNS软件和服务的操作以及DNS区管理制定指南。
- 工作职责
  - 描述域名系统（DNS）软件可在Internet网络上高效、正确地管理、配置和操作的实践。
  - 发布有关DNSSEC操作程序的文件。
  - 发布有关IPv6和IPv6-IPv4混合网络中DNS操作过程的文档，并提供与DNS相关的IPv6转换和共存问题的文档和指导。

Domain Name System Operations (dnsop)

- 工作职责
  - 通过对DNS协议进行扩展或执行协议维护，解决DNS协议的操作问题。例如EDNS0选项、新的RRTYPE、DNSSEC或其他扩展DNS以支持其他应用程序的机制。
  - 记录现有的或新的DNS问题。
- Chairs
  - Benno Overeinder (NLnet Labs)
  - Suzanne Woolf (Internet Systems Consortium, Inc.)
  - Tim Wicinski

Domain Name System Operations (dnsop)

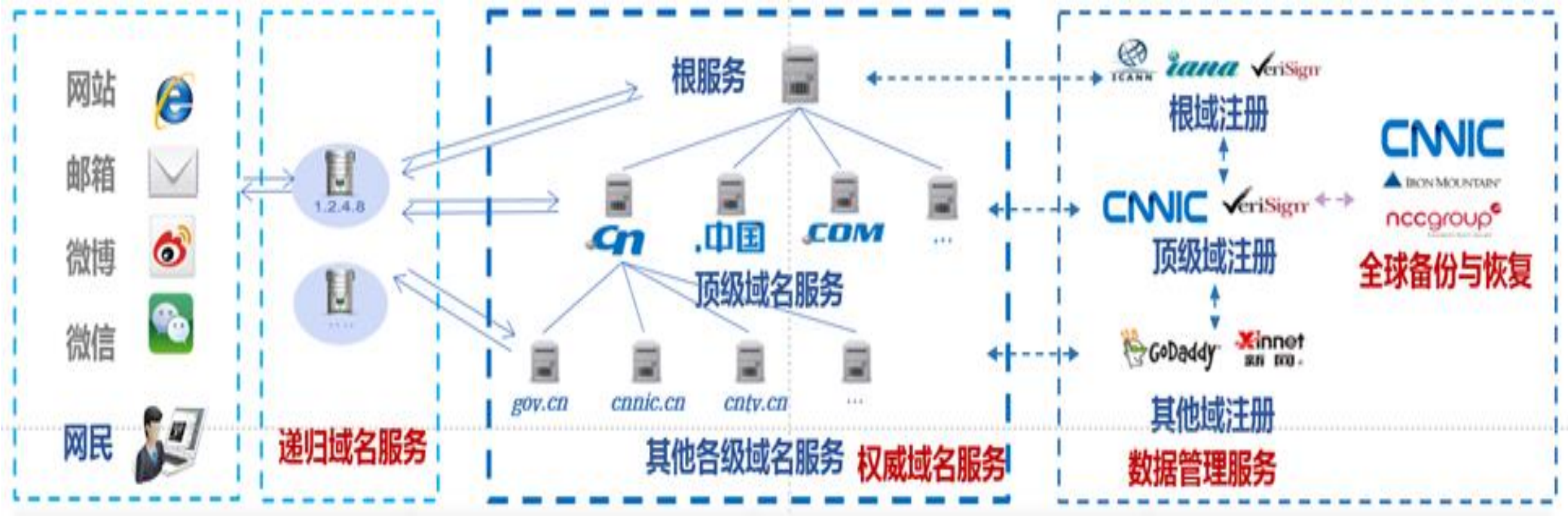
已发布RFC（59篇）
RFC 9108 YANG Types for DNS Classes and Resource Record Types
RFC 9077 NSEC and NSEC3: TTLs and Aggressive Use
RFC 9018 Interoperable Domain Name System (DNS) Server Cookies
RFC 8976 Message Digest for DNS Zones
RFC 8945 Secret Key Transaction Authentication for DNS (TSIG)
RFC 8914 Extended DNS Errors
RFC 8906 A Common Operational Problem in DNS Servers: Failure to Communicate
RFC 8901 Multi-Signer DNSSEC Models
RFC 8806 Running a Root Server Local to a Resolver
RFC 8767 Serving Stale Data to Improve DNS Resiliency
RFC 8749 Moving DNSSEC Lookaside Validation (DLV) to Historic Status
RFC 8624 Algorithm Implementation Requirements and Usage Guidance for DNSSEC

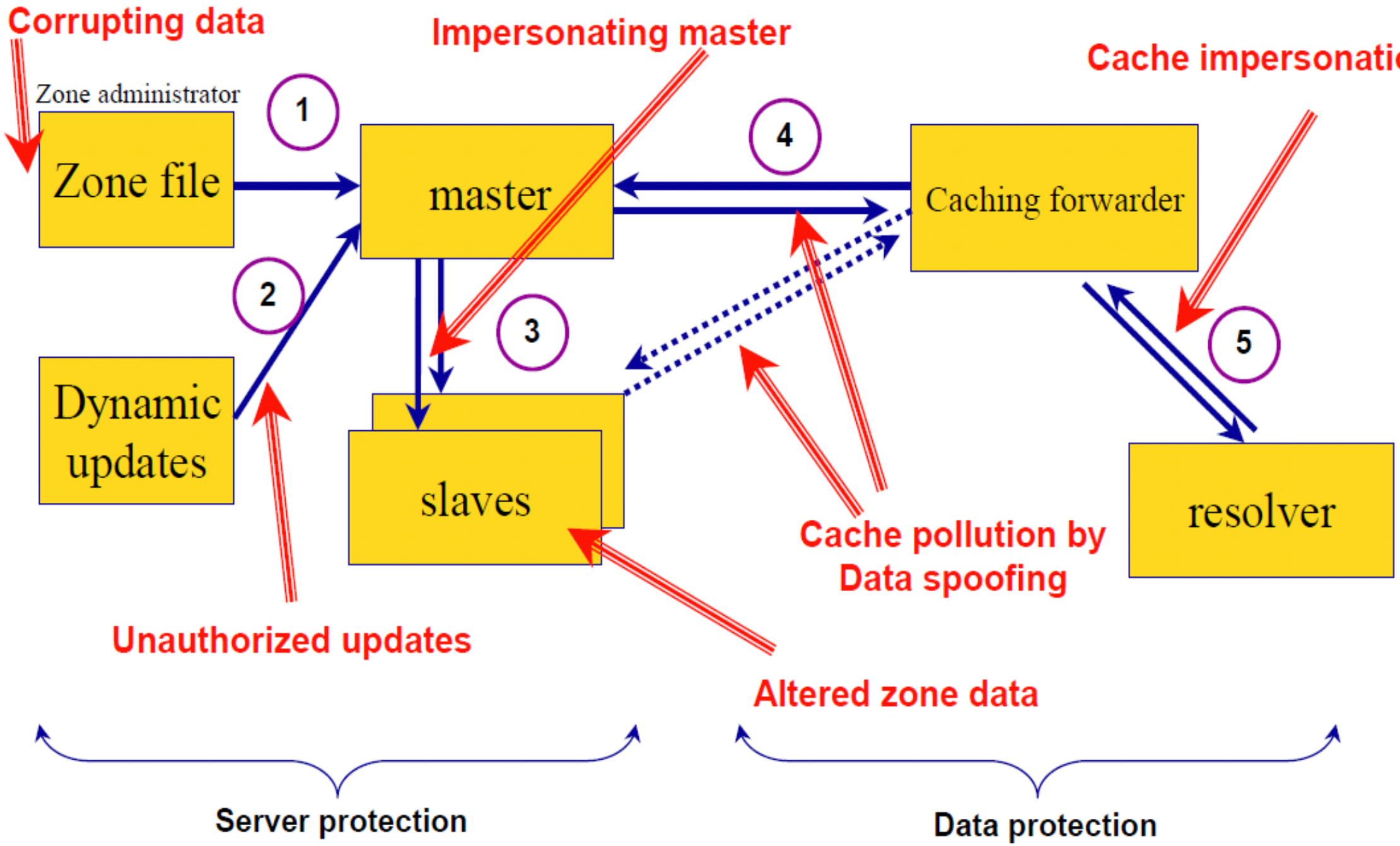
Domain Name System Operations (dnsop)

Active Internet-Drafts（15篇）
The ALT Special Use Top Level Domain
DNS Transport over TCP - Operational Requirements
Revised IANA Considerations for DNSSEC
DNS Query Name Minimisation to Improve Privacy
DNS Terminology
Service binding and parameter specification via the DNS (DNS SVCB and HTTPS RRs)
Fragmentation Avoidance in DNS
DNS Catalog Zones
DNS Error Reporting
Glue In DNS Referral Responses Is Not Optional
Delegation Revalidation by DNS Resolvers
Guidance for NSEC3 parameter settings

DNS相关工作

- 斯诺登前--》DNSOP和 DNSEXT
- 斯诺登后--》DOH DOT DOQ




Corrupting data
Impersonating master
Cache impersonation
Zone administrator
1
Zone file
master
4
Caching forwarder
2
3
5
Dynamic updates
slaves
resolver
Cache pollution by Data spoofing
Unauthorized updates
Altered zone data
Server protection
Data protection

DNS PRIVate Exchange (dprive)

- 个人发出的一组DNS请求可以向攻击者提供有关该个人的大量信息。DPRIVE工作组致力于开发为DNS提供保密性的机制。
- 该工作组最初的重点是开发在DNS客户端和递归解析器之间提供机密性和身份验证的机制，随着DoT和DoH的发布，工作重点进行了转移。
- 使用递归解析器的DNS交互和涉及DNS根/权威服务器的交互之间，存在许多不同的方面。工作组将与DNS运营商和开发者（通过DNSOP工作组）合作，以确保提议的解决方案满足关键要求。
- **Chairs**
  - **Brian Haberman (**Johns Hopkins University**)**
  - **Tim Wicinski**

DNS PRIVate Exchange (dprive)

- 工作内容
  - 为DNS提供机密性的机制，随着客户端到递归解析器之间加密的RFC发布，工作组的重点转移到了以下的方向：
  - 制定要求，为递归解析程序和权威服务器之间的DNS交互增加机密性；
  - 研究为关于权威服务器的DNS交互增加机密性的潜在解决方案（实验性）；
  - 定义、收集和发布性能数据，测量保护隐私方法的有效性；
  - 为提供DNS隐私服务的DNS运营商定义运营，策略和安全注意事项；
  - 记录操作 DNS 隐私服务的当前最佳实践。

DNS PRIVate Exchange (dprive)

已发布的RFC（9篇）
RFC 7626 **DNS Privacy Considerations**
RFC 7830 **The EDNS(0) Padding Option**
RFC 7858 **Specification for DNS over Transport Layer Security (TLS)**
RFC 8094 **DNS over Datagram Transport Layer Security (DTLS)**
RFC 8310 **Usage Profiles for DNS over TLS and DNS over DTLS**
RFC 8467 **Padding Policies for Extension Mechanisms for DNS (EDNS(0))**
RFC 8932 **Recommendations for DNS Privacy Service Operators**
RFC 9076 **DNS Privacy Considerations**
RFC 9103 **DNS Zone Transfer over TLS**

DNS PRIVate Exchange (dprive)

Active Internet-Drafts (2 hits)
Specification of DNS over Dedicated QUIC Connections
Recursive to Authoritative DNS with Unauthenticated Encryption

Related Internet-Drafts (5 hits)
Authenticated DNS over TLS to Authoritative Servers
DNS over HTTPS via HTTP proxies
Oblivious DNS Over HTTPS
Common Features for Encrypted Recursive to Authoritative DNS
Nameserver Access Modes with Encryption Held in Alphanumeric Configuration Keys

Adaptive DNS Discovery (add)

- 按照DoT（RFC 7858）和DoH（RFC 8484）中的定义，通过加密传输发送DNS消息有利于DNS数据的安全性和隐私性。
- 该工作组将重点关注DNS客户端在各种网络环境中发现和选择DNS解析器，包括公共网络、专用网络和VPN，支持加密和未加密的解析器。
- 采用加密DNS协议的客户端需要确定哪些DNS服务器支持这些协议，如果有多个服务器可用，则需要确定用于特定查询的服务器。这些决策可能因网络环境以及客户端查询的内容和目的而异。
- 在服务器上支持DNS加密的网络运营商也需要一种方法来告诉客户端。通过交互有关解析器配置和行为的信息，客户端可以对使用哪些DNS服务器做出更明智的决定。
- **Chairs**
  - **David Lawrence (Salesforce)**
  - **Glenn Deen (Comcast-NBCUniversal)**

Adaptive DNS Discovery (add)

- ADD工作组的议题方向主要包括以下几个方向：
  - 定义一种机制，允许客户端发现支持加密的DNS解析器，这些解析器可供客户端在公用Internet或专用或本地网络上使用。
  - 定义一种机制，允许将DNS解析器信息通信给客户端，以便在选择决策中使用。这可能是上述发现机制的一部分。
  - 开发一份信息文档，描述客户端检测特定网络环境（如captive portal和split horizon）的机制，并使用该信息通知其DNS配置。
  - 该工作组将与dnsop、doh和dprive协调DNS协议中所需的任何更改，并确保在适当的时候将这些组包括在主要文件review中。

Adaptive DNS Discovery (add)

暂时没有已发布的RFC

Internet-Drafts
Discovery of Designated Resolvers 定义了一种在现有非加密解析器的基础上发现加密解析器的机制
DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR) DHCP 和路由器通告选项升级以支持加密解析器的发现
Split-Horizon DNS Configuration
Service Binding Mapping for DNS Servers
Analysis of DNS Forwarder Scenario Relative to DDR and DNR
Discovery of Encrypted DNS Resolvers: Deployment Considerations
Analysis of DNS Forwarder Scenario Relative to DDR and DNR
Internet Key Exchange Protocol Version 2 (IKEv2) Configuration for Encrypted DNS
DNS Resolver Information
DNS Server Selection: DNS Server Information with Assertion Token

Q&A