International Telecommunication Union

ITU-T Technical Paper

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(03/2020)

XSTP-ORS

OID resolution system: Problems, requirements and potential solutions

Summary

This Technical Paper identifies problems, requirements and potential solutions for OID resolution. The problems include local performance and global resolution of missing OID subtrees. Technical requirements for possible solutions are also discussed. Finally, potential technical solutions, administrative and operational guidance are provided.

Keywords

OID missing nodes, OID resolution, ORS, performance.

NOTE – This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Table of Contents

Technical Paper ITU-T XSTP-ORS

OID resolution system: Problems, requirements and potential solutions

1 Scope

This Technical Paper identifies the challenges in current implementations of OID resolution, defines the requirements for meeting those challenges and proposes technical, operational and administrative solutions that would address these requirements.

The scope of the Technical Paper is:

1) to identify problems related to the local performance of OID resolution, as well as operational issues observed in the ORS;
2) to identify problems associated with missing elements of OID subtrees where organizations and entities have OID services in operation but where parts of the subtree above those entities do not implement OID resolution;
3) to identify the technical, operational and administrative requirements for meeting the challenges identified in 1) and 2) above;
4) to propose technical, operational and administrative solutions that can be used to meet the requirements in 3) above (part of the intent of the Technical Paper is to provide useful and practical operational guidance for operators of OID resolution services);
5) to identify, if necessary, any future standardization work that needs to be completed to assist in meeting the goals of improvements in the operation and performance of OID resolution.

2 References

All Recommendations and other references are subject to revision; users of this Technical Paper are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below.

[ITU-T X.660] Recommendation ITU-T X.660 (2011) | ISO/IEC 9834-1:2012, *Information technology – Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree*.

[ITU-T X.672] Recommendation ITU-T X.672 (2010) | ISO/IEC 29168-1:2011, *Information technology – Open systems interconnection – Object identifier resolution system (ORS)*.

[ISO/IEC 29168-2] ISO/IEC 29168-2:2011, *Information technology – Open systems interconnection – Part 2: Procedures for the object identifier resolution system operational agency*.

[IETF RFC 2182] IETF RFC 2182 (1997), *Selection and Operation of Secondary DNS Servers*. <https://www.rfc-editor.org/info/rfc2182>

[IETF RFC 6672] IETF RFC 6672 (2012), *DNAME Redirection in the DNS*. <https://www.rfc-editor.org/info/rfc6672>

[IETF RFC 7706] IETF RFC 7706 (2015), *Decreasing Access Time to Root Servers by Running One on Loopback*. <https://www.rfc-editor.org/info/rfc7706>

3 Terms and definitions

For the purposes of this document, the following definitions apply:

– **application-specific OID resolution process** [ITU-T X.672]: Actions by application to retrieve application-specific information from the information returned by the general OID resolution process.

– **AXFR** [b-IETF RFC 5936]: DNS zone transfer protocol.

– **DNS resource record** [based on b-IETF RFC 1035]: A component of a DNS zone file.

– **DNS zone file** [based on b-IETF RFC 1035]: A text file that describes a portion of the DNS.

– **general OID resolution process** [ITU-T X.672]: That part of the ORS where an ORS client obtains information from the DNS (recorded in a zone file) about any specified OID and returns it to an application.

– **object identifier** [ITU-T X.660]: An ordered list of primary integer values from the root of the international object identifier tree to a node, which unambiguously identifies that node.

– **OID local resolution**: Local OID resolution interface through which the cached ORS-supported DNS record is retrieved locally.

– **OID resolution system (ORS)** [ITU-T X.672]: Implementation of the OID resolution process.

– **QNAME minimization** [based on b-IETF RFC 7816]: A technique to change the DNS queries (query name) from the recursive resolver to include only as much detail in each query as is required for that step in the resolution process.

– **registration authority** [ITU-T X.660]: An entity such as an organization, a standard or an automated facility that performs registration of one or more types of objects.

– **RRset** [b-IETF RFC 8499]: A set of DNS resource records "with the same label, class and type, but with different data".

4 Abbreviations and acronyms

This Technical Paper uses the following abbreviations and acronyms:

APP	Application
CNAME	Canonical Name Record or Alias Record
DLV	DNSSEC Lookaside Validation
DNS	Domain Name System
DNSSEC	The Domain Name System Security Extensions
ENUM	ITU-T E.164 to URI (uniform resource identifier) mapping
FQDN	Fully Qualified Domain Name
HTTPS	Hypertext Transfer Protocol Secure
IoT	Internet of Things
IP	Internet Protocol
NAPTR	Naming Authority Pointer
NS	Name Server
OID	Object Identifier
ORS	OID Resolution System

P2P	Peer-to-Peer
sFTP	secure File Transfer Protocol
SLA	Service Level Agreement
SOA	Start of a Zone of Authority

5 Conventions

None.

6 Problem analysis

[ITU-T X.672] specifies the object identifier (OID) resolution system (ORS). This system allows for any arbitrary information to be associated with any ORS-supported OID node (as specified in [ITU-T X.660]). [ITU-T X.672] specifies that the OID tree is to be mapped into a part of the public domain name system (DNS) tree with the root of the OID tree mapped into `.oid-res.org`.

In practice this mapping has an important pair of challenges: first, the authoritative zone for this mapping needs to be configured correctly for proper performance; and second, management of the `.oid-res.org` zone needs to be made easier.

This Technical Paper identifies the key performance and management problems of the existing ORS, and makes recommendations to improve the performance and management of the existing ORS.

6.1 Performance issue

The ORS takes advantage of DNS properties, such as ubiquity and scalability. However, the nature of the OID tree is not typical of public uses of the DNS. One difference is the depth of the OID's hierarchical name structure. In the DNS, the second level domain is very popular and used widely. However, in the OID tree, the depth of OID may surpass 10 levels, including the suffix name `oid-res.org`. For example, the OIDs beneath the node of Cisco's Management Information Bases (`1.3.6.1.4.1.9.9`) are considered to represent nearly 6% OIDs of all allocated OIDs.

Very deep hierarchies for the DNS have been implemented for other purposes. For instance, the ITU-T E.164 to URI mapping (ENUM) maps standard phone numbers into the DNS. ENUM allocates a specific zone, specifically "`e164.arpa`" for use with ENUM ITU-T E.164 numbers on the IP side of the network. [b-IETF RFC 6116] defines how any ITU-T E.164 number, such as +1 555 42 42, can be transformed into a URI, by reversing the numbers, separating them with dots and adding the `e164.arpa` suffix thus: `2.4.2.4.5.5.5.1.e164.arpa`. Like OIDs, ENUM represents a use case of the DNS where a very deep hierarchical namespace is effectively represented in the DNS with proper administration and management of DNS hierarchy.

A key problem for ORS-supported OID nodes is that their authoritative servers are not well configured, sometimes due to a lack of expertise, human resources or network resources. So, there are noticeable performance issues in the ORS in terms of service availability and response latency. Misconfiguration, or insufficient human or network resources increase the possibility of failure and operational issues in the chain of the ORS. This, in turn, impacts the stability of the resolution process. As shown on Figure 1, any failure of OID `x.y` will impact OID `x.y.z`.

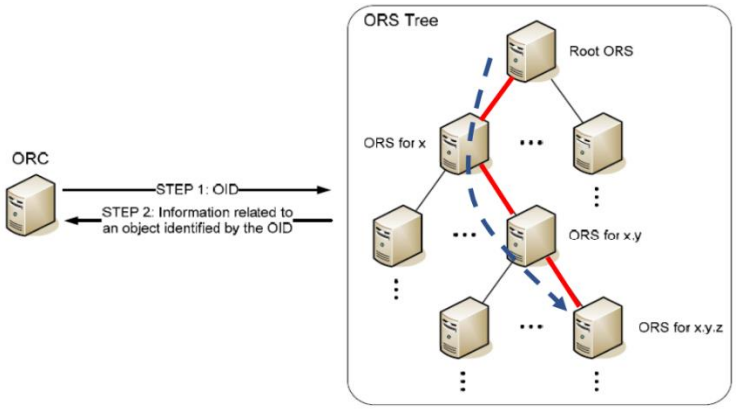

Figure 1 – The deep depth of OID resolution caused by the OID hierarchy

The OID resolution system (ORS) is not only used for the purpose of static information retrieval. It is also integrated into a resolution system for the purpose of online hosts and real-time communications with performance requirements [ITU-T X.675] and [ITU-T X.676]. The performance should be enhanced to be ready for real-time communication in production networks.

There is plenty of experience and best practice in DNS operations for dealing with these issues. Like any normal DNS operation, ORS operators (especially for `oid-res.org`) should follow and adopt the best practice of DNS operation using secondary DNS. On the client side, ORS client implementers should consider using special cache mechanisms instead of traditional local DNS caches. In clause 8.1, solutions are proposed using DNS best practices on both the server side and the client side according to different scenarios.

6.2 Global resolution of missing OID subtrees

The ORS was proposed in 2010 and deployed many years after the concept of OID was standardized. ORS support for an OID node is not strictly required when an OID is registered or maintained. In particular, some intermediate registration authorities do not support the ORS. Some examples are listed in Table 1.

However, the DNS zone files for the `.oid-res.org` domain are managed in a way where a complete ORS hierarchy is required for an OID to support the ORS. In clause 6.1.4 of [ITU-T X.672], it is specified that, if the OID node is ORS-supported, its parent OID node is required to be ORS-supported. According to clause 6.1.3 of [ITU-T X.672], if the OID node is not ORS-supported, its child OID nodes cannot be ORS-supported.

In this case, the requirement for a complete ORS-supported hierarchy for any OID node becomes a problem for OID resolution. For example, in the current implementation, if one arc in the chain does not implement the ORS all subsequent arcs cannot use the ORS at all.

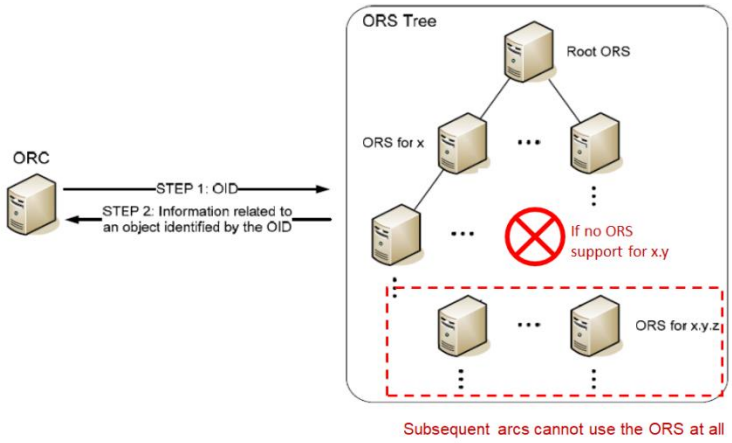

Figure 2 – The situation of lack of ORS support in the OID tree

As shown in Figure 2, if the registration authority for OID `x.y` does not implement the ORS, any arc beneath `x.y` will not be resolvable by the ORS. This situation is not rare and many important OIDs cannot use the ORS (see Table 1).

Table 1 – Examples of OIDs which are not resolvable by the ORS

OID	Application field	Available in the ors?
2.49.0	World Meteorological Organization (WMO)	No
1.2.840.113549.1.19.16.3.27	AES with SIV CMACwrap 512 bits	No, 1.2.840 is missing
1.3.6.1.4.1.36906.5.3.1	Bimodal LattIce Signature Scheme (BLISS) with SHA2-512 hash function	No, 1.3.6 is missing
2.16.840.1.113883	E-health, HL7 international	No, 2.16.840 is missing
1.3.6.1.6.3.13	Management information bases (MIBs) for the Simple Network Management Protocol (SNMP)	No, 1.3.6 is missing
2.5.29.32	ITU-T X.500 certificate policies	No, 2.5.29 is missing
2.1.5	XER (XML Encoding Rules for ASN.1)	No
1.2.156.3001.3851	OID of household electrical appliances by Haier Digital	No, 1.2.156.3001 is missing

Like ENUM, the ORS needs a mechanism to provide authoritative zones for parts of the OID tree that have missing "intermediate" nodes. This is a separate problem from the performance issue: It is essentially a problem for the management and administration of the zones in the `oid-res.org` domain. Using existing technology and the experience gained from mapping telephone numbers onto the DNS, it is possible to use the fundamental features of the ORS while supporting those OIDs with arcs which are not yet in an authoritative zone.

6.3 Other issues

It is also clear that there are operational issues in the OID root zone (`oid-res.org`). For example, the two ORS root servers `ns1.oid-res.org` (IP: 202.30.45.1) and `ns2.oid-res.org` (IP: 202.30.45.2) are located in the same /24 network. This is contrary to best operational principles for the DNS.

7 Requirements analysis

In this clause, technical, operational and administrative requirements for meeting these challenges are proposed.

7.1 Requirements for the performance issue

There are two major performance issues for the ORS described in the previous clause: high latency (response time up to full seconds) and low availability. For the ORS to be successful, both the latency and availability issues need to be addressed. In this Technical Report, we suggest that the ORS should have performance and availability characteristics that match other important infrastructure facilities on the public Internet. Considering the state of art in the DNS field, it is a best practice for DNS services to achieve query speeds of less than 100 milliseconds and uptime greater than 99% [1].

Servers that provide resources for the ORS should be able to handle a large number of requests to that zone three times the measured peak of such requests currently measured. Connectivity to the Internet should be as diverse as possible. The ORS servers should provide authoritative responses only for the zones they serve. The ORS servers should disable recursive lookup, forwarding or any other function that may allow them to provide cached answers. The servers must answer queries from any Internet host and not block ORS resolution from any valid IP address.

7.2 Requirements for the global resolution of missing OID subtrees

In the current ORS, some intermediate OID nodes do not deploy the ORS. As a result, OIDs below those nodes are not resolvable in the current system. What is needed is an administrative and technical solution that makes it possible to resolve any OID node using the ORS even if intermediate nodes have not deployed or implemented the ORS.

7.3 Security requirements

Any new technical solution or operational changes should not introduce new security threats or flaws. A security evaluation during the design and implementation of any changes to the ORS should be a fundamental part of addressing ORS deployment issues.

7.4 Other requirements

Any improvements to the current ORS should also address the following requirements:

1) Support for incremental deployment: Any new technical solution or operational changes should support incremental deployment so that early adopters do not need to rely on others and gain immediate benefit of it. It will encourage and enable OID subtrees to opt in any newly proposed technical solution or operational changes.
2) Low impact on the current ORS: For any operational system, it is required that the impact and changes to the current ORS is as less as possible.
3) Adaptability: For any improvement to the ORS, flexibility must be in place to take advantage of new DNS technologies that might improve performance, privacy or security.
4) While it is not clear that the root of the ORS should be signed, other measures for security and privacy in the evolving DNS should be considered for implementation (for instance, support for DPRIVE[2]).

---

1 https://www.dnsperf.com/

2 See IETF DNS DPRIVate Exchange (dprive) Working Group.

8 Technical solutions

8.1 Technical solutions for the performance issue

8.1.1 Selection and operation of secondary ORS servers

There are lots of experience and best practices in DNS for performance and availability issues. For example, [IETF RFC 2182] introduces the selection and operation of secondary DNS servers.

As introduced in [IETF RFC 2182], a number of problems in DNS operation today are attributable to poor choices of secondary servers for DNS zones. Take the example of the OID root zone (`oid-res.org`), the two ORS root servers, `ns1.oid-res.org` (IP: 202.30.45.1) and `ns2.oid-res.org` (IP: 202.30.45.2), are located in the same LAN segment. It is a bad practice for the DNS.

A good selection of a secondary server for a zone with geographic placement, as well as the diversity of network connectivity, can increase the reliability of that zone as well as improve overall network performance and access characteristics.

8.1.2 Local cache for OID resolution

In addition to name server operation, the cache managed by the DNS resolver is another effective means to reduce the response time. However, in the case of the ORS, the DNS resolver may be out of the control of ORS client users (for example the DNS resolver provided by local ISP). It is very hard to adopt cache strategy in a local ISP resolver.

An ORS client is able to maintain a cache of popular OIDs by itself by pre-configuration or by learning from the recent OID resolution process. The cache can be kept warm by periodically fetching according to their TTL.

A typical use case is in IoT grouped services introduced in [ITU-T X.676]. When an emergency (i.e., accident) occurs and people make the call for "Emergency Service" (e.g., 2.999.1.1) based on an OID resolution, the ORS client can respond promptly from the cache. In addition, it also increases the resilience of OID resolution against network failure.

8.1.3 Local copies of ORS zones

Another approach serving ORS information locally is to provide private copies of ORS zones frequently used when resolving OIDs. An example use case is in a vertical industry (for instance, medical devices) where a single node of the DNS subtree might contain many arcs of interest to a specific application using OIDs.

An application doing OID resolution is required to do two steps: first, upon acceptance of a query for information from the ORS, the application constructs a DNS query for the FQDN. This FQDN is submitted to the ORS DNS server in the usual way. In addition, the ORS client also submits an AXFR (252) query to the ORS zone to initiate a zone transfer for the root of the related OID. The system relies entirely on existing DNS technology but requires the ORS client to issue both standard queries and requests for zone transfer for zones related to commonly used arcs.

The advantage of the solution in this clause is that it solves the problem of local caching of the ORS-related Naming Authority Pointer (NAPTR) [b-IETF RFC 2915] records by having the DNS client initiate a zone transfer for related ORS records. The primary disadvantage is that it relies on the local operator of the local resolver to be configured to issue AXFR zone transfers for zones related to the query that was issued on behalf of the ORS. While this can be done entirely in the DNS, it may not reflect the general use case where a large number of zones is required – outside of the zone being transferred for the specific query.

8.1.4 Local copies of ORS zones independent of local DNS

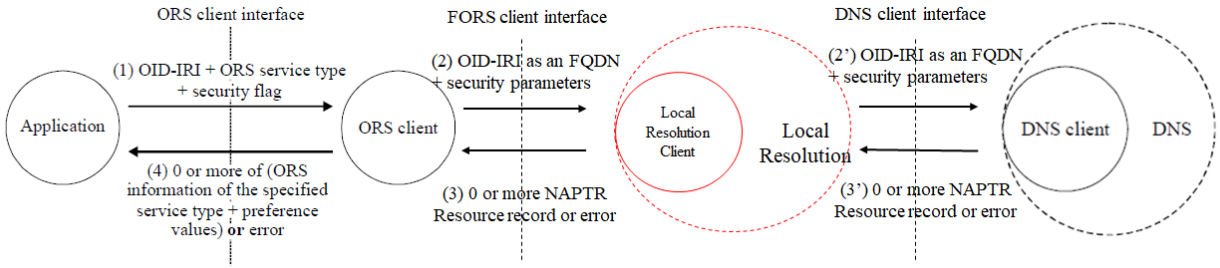

Figure 3 – General OID resolution process including a local root component

In clause 8.1.3, the local copy of ORS zones is an internal component in the DNS client. Alternatively, the function can also act as an independent actor outside of the DNS client as shown in Figure 3, which is called Local Resolution. It is composed of a DNS authoritative server and a DNS resolver (Local Resolution client) running on the same host. The Local Resolution can cache and slave the important zone locally as specified in [IETF RFC 7706].

NOTE – [IETF RFC 7706] was firstly defined to slave the root zone locally to reduce the response latency and provide more reliable answers for queries to the root. Although the primary goal of the design is for serving the root zone, the method can be used for any zone.

Let's suppose an important zone, `example.oid-res.org`, is going to be slaved locally. The operation of `example.oid-res.org` on the Local Root client is described as follows:

1) Retrieve a copy of the zone of `example.oid-res.org` from its name server.

   NOTE – If the OID root zone is going to be hosted locally, the zone of oid-res.org should be retrieved.

2) Start the authoritative service for `example.oid-res.org`.

The contents of the `example.oid-res.org` zone shall be refreshed using the timers from the SOA record in the zone file. In a resolver that is using an internal service for the `example.oid-res.org` zone if the contents of the zone cannot be refreshed before the expiry time in the SOA, the resolver shall immediately switch to forward the query to the standard DNS resolver.

In this design, the Local Resolution should switch to forward the query to the normal DNS client if the local authoritative server defined in [IETF RFC 7706] has failed.

8.1.5 Comparison of the four approaches for the performance issue

– **Solution proposed in clause 8.1.1**

The advantage of this solution is that it is a common practice to add multiple servers for ORS services. It is easy to find DNS operators in the market who can help to host the secondary DNS server for particular ORS zones. Large managed DNS operators can provide good service level agreements (SLAs) for ORS. This is recommended in clause 10.1. The only concern is that it requires the action from operators for particular ORS zones.

– **Solution proposed in clause 8.1.2**

The advantage of this solution is that it solves the problem of local caching of the ORS related NAPTR records by normal queries by the client without the coordination from the serve side. The ORS client can adopt different local policy to pre-cache the selected important OID and control the size of the cache. The cost of this solution is the modification of the ORS client.

– **Solution proposed in clause 8.1.3**

The advantage of this solution is that it fits the situation if there is a bulk of OIDs contained in a zone interest to a specific application using OIDs. To support this function, it requires the operator of that

ORS zone to open DNS zone transfer service publicly. It is OK for small zones like `oid-res.org`, but may be a burden for large zones containing millions of names.

In addition, it relies on the local operator of the local resolver to be configured to issue AXFR zone transfers for zones related to the query that was issued on behalf of the ORS. It is not easy to coordinate the local resolver from the local ISP or publish the DNS server.

– **Solution proposed in clause 8.1.4**

The advantage of this solution is the same as in clause 8.1.3. In addition, it does not rely on the local operator because the Local Resolution component is implemented outside of the DNS client. The cost of this proposal is to implement a Local Resolution component cooperated with the ORS client.

8.2 Technical solutions for missing OID subtrees

To support those OIDs with arcs which are not yet in an authoritative zone, operational changes are proposed on the ORS authoritative server side. In general, there are two potential approaches: one is to publish and sign the missing OID nodes in one authoritative zone; another is to place these functions in a superior ORS-supported node for each missing OID node.

8.2.1 Publish and sign all missing OID nodes in one authoritative zone

Similar to the DNSSEC DLV defined in [b-IETF RFC 5074], another domain `oid-res2.org` is chosen to publish and sign the DNS zone information for each missing OID node. A new ORS tree from `oid-res2.org` serves as a supplementary tree to the current ORS tree which starts from `oid-res.org` as show in Figure 4.

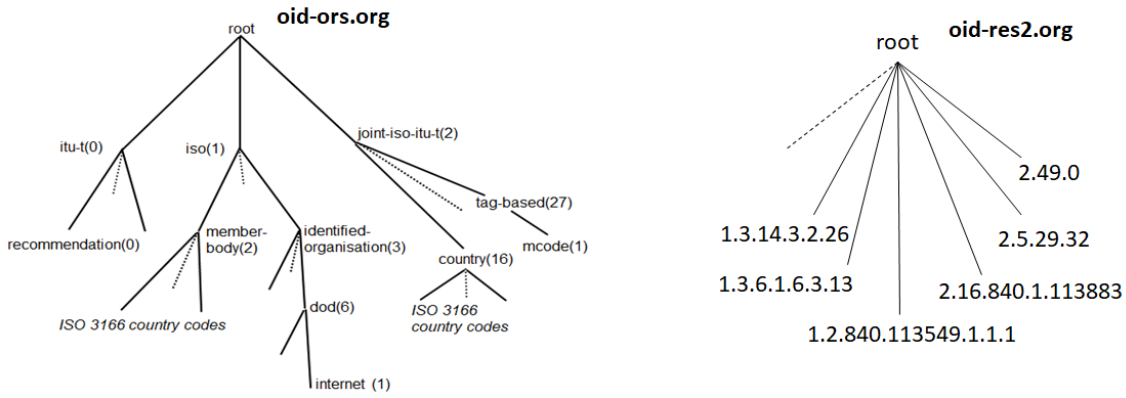

Figure 4 – Current ORS root and a supplementary ORS root

If OID `2.5.29.32` is willing to support the ORS, `oid-res2.org` is used to publish and sign the zone information of `32.29.5.2.oid-res2.org` in a DNS domain format.

To redirect the DNS queries to `oid-res2.org`, a DNAME [IETF RFC 6672] is used to redirect all names that end with the suffix `exmaple.oid-res1.org` to `example.oid-res2.org`. For example, the DNAME record of `32.29.5.2.oid-res2.org` is `32.29.5.2.oid-res2.org` if the ORS record of OID `2.5.29.32` is registered and published in the `oid-res2.org`.

Note that the DNAME of `32.29.5.2.oid-res.org` should not be configured in the zone of `oid-res.org` which breaks the possible existing delegation of `5.2.oid-res2.org`. A possible implementation is to place a function component in front of the name server of `oid-res.org` which captures the query of a missing OID node and responds with a proper DNAME.

This approach is efficient in a centralized style to redirect the query for the missing OID nodes. It uses the existing DNS DNAME technology [IETF RFC 6672] and easily monitors the process on which OIDs and how many of them are resolvable in the ORS based on this solution. However, it

requires modifications on the ORS root by keeping track of registered missing OID nodes and responding with the DNAME records accordingly.

Another notable drawback of this approach is that it is impacted by QNAME minimization provided by many DNS resolvers. Indeed, if the DNS resolver adopts QNAME minimization, the ORS root may not receive queries with the full query name of missing OID nodes.

8.2.2 Publish and sign each missing OID node in a superior ORS-supported node

Another approach is to change the way of management and administration of DNS zones for the `oid-res.org` domain. More specifically, it is reasonable to lose the requirement in clause 6.1.4 of [ITU-T X.672], i.e., if one OID node is ORS-supported, the parent OID node is required to be ORS-supported. As introduced in clause 6.2, it is a normal practice for a DNS zone to contain authoritative data of a domain name (with one or more labels) as long as there is no zone cut (delegation) for a label in the middle of that name. (An example is given in Annex A.)

According to that approach, it is required that an ORS-supported OID node is able to provide authoritative data for any missing OID node which is beneath that OID node. For the case of a missing OID node, there is no zone cut for its parent which required ORS support. In this case, any OID node whose parent is not ORS-supported can still implement the ORS with the help of its superior ORS-supported node. The superior ORS-supported node shall determine by mutual agreement whether that OID node become ORS-supported.

For example, OID `2.5.29.32` is not ORS-supported because its superior OID `2.5.29` is not ORS-supported. In theory, the registration authority of OID `2.5` can publish the OID zone information of OID `2.5.29.32` instead of waiting for OID `2.5.29` to support the ORS. However, OID `2.5` is administered directly by the ORS root according to [ISO/IEC 29168-2], so in the case of OID `2.5.29.32`, its OID zone information should be published by the ORS root (`res-oid.org`) to achieve the goal.

This approach is based on existing DNS technology and practice, and resolves the issue in a distributed style. It requires modification of [ITU-T X.672] to adopt a flexible zone management in the ORS. Although it involves more coordination between each missing OID node and their superior ORS-supported node, the early adopters benefit from it immediately.

8.2.3 Publish and sign all missing OID nodes in a cloud database

It is also proposed to adopt cloud and database technologies to resolve issues in OID resolution. A cloud database can definitely serve the role because there is no name hierarchy limitation in the database and the performance of the OID resolution can be enhanced by the cloud (content delivery network, for example).

It is also observed that there is a momentum about application-level DNS in which applications do DNS resolving on ports 80 and 443.

Either way, it requires major modification on both the ORS client and server, or setting up an alternative system to work in parallel with the current ORS. It does not meet the requirement of "Low impact on the current ORS" in clause 7.4.

8.2.4 Comparison of three server-side approaches

– Solution proposed in clause 8.2.1

The advantage of this solution is the efficiency to register and publish the ORS records of and missing OID in one place. The cost is that it requires modification of the ORS root with a special response loop to handle queries for missing OIDs. In addition, the QNAME minimization adopted by the DNS resolver may have impact on this solution.

– **Solution proposed in clause 8.2.2**

The advantage of this solution is that it is based on existing DNS technology and practice. It only adjusts the management and administration of the zones in the `oid-res.org` domain which still relies on fundamental features of the ORS. To support that, it requires modification of [ITU-T X.672] to adopt a flexible zone management in the ORS. This is recommended in clause 10.3.

– **Solution proposed in clause 8.2.3**

The solution proposed in this clause is to use a clean-slate approach to design a new OID resolution system with the latest cloud and database technologies, and transform the DNS-based ORS into a web service. However, it is out of the scope of the ORS, and requires human resources and time to achieve the goal. Currently, no strong motivation or sufficient resources are observed in the OID community on supporting this proposal. If there is enough resource and motivation in the future, people can utilize the latest cloud and database technologies for the OID resolution.

In conclusion, all technical solutions are listed and compared in Table 2.

Table 2 – Comparison among the technical proposals

Solutions in clause	Problem it solves	Brief introduction	Cost evaluation	Recommended?
Solution in clause 8.1.1	Performance issue	Best practices of DNS	With more servers and little impact to ORS	Yes
Solution in clause 8.1.2	Performance issue	Warm cache on ORS client	Require changes on ORS client	Yes
Solution in clause 8.1.3	Performance issue	Local copies of ORS zones	Need coordination and help of local resolver operator	Depends on the situation
Solution in clause 8.1.4	Performance issue	Local copies of ORS zones	Require changes on ORS client	Depends on the situation
Solution in clause 8.2.1	Missing OID nodes	Special design on ORS root to redirect the query to another zone	Require changes on ORS root and impacted by QNAME minimization	No
Solution in clause 8.2.2	Missing OID nodes	Publish and sign each missing OID node in a superior ORS-supported node	Require changes on current ORS zone management	Yes
Solution in clause 8.2.3	Performance issue and missing OID nodes	Build another OID resolution services using cloud and database technologies	Need motivation and resources to work on this proposal	Not now but may be in the future

9 Administrative and operational guidance

Guidance on implementation, administration and operation of ORS is given.

– ORS operators should check and follow the best practice of DNS to operate the ORS. It is suggested that ORS operators cooperate with DNS operators to provide an SLA for the ORS service.

– To reduce the ORS response time and enhance its performance, it is strongly suggested to deploy more secondary servers in different geographic locations to serve the ORS root zone and other important ORS zones.
– ORS-supported zones which are willing to be "subscribed" by the Local Resolution of an ORS client can publish the update-to-date zone public accessible. For example, the `example.oid-res.org` name server should open the access of the ORS zone file via DNS zone transfer, web service or a P2P file-sharing network, the Local Resolution can retrieve it via HTTPS or sFTP.
– A monitoring system should be designed and set up to periodically evaluate new adopted solutions and the status quo of the challenges analyzed in clause 6.

10 Recommendations

10.1 Recommendation 1

According to clause 8.1.1, in order to enhance the performance and high availability of the ORS root (`oid-res.org`), it is highly recommended that the ORS operational agency shall implement more secondary DNS servers by DNS operators. It also applies to any ORS zones who want to enhance their ORS performance.

10.2 Recommendation 2

According to clause 8.1.2, in order to reduce the response time in the client side, the ORS client can cache the ORS related NAPTR records locally or provide private copies of popular ORS zones when resolving OIDs.

NOTE – Clauses 8.1.2, 8.1.3 and 8.1.4 are implementation options for the ORS client. They are not mandatory and OID application implementers can take a decision depending on their situation.

10.3 Recommendation 3

According to clause 8.2.2, any OID node whose parent is not ORS-supported can implement the ORS with the help of its superior ORS-supported node. The superior ORS-supported node shall determine by mutual agreement whether that OID node become ORS-supported. It requires changes to the current ORS zone management defined in [ITU-T X.672].

10.4 Recommendation 4

According to clause 8.2.3, if there are enough resources and motivation in the future, it is recommended to utilize the latest cloud and database technologies for OID resolution.

11 Potential requirement for future standardization

11.1 Proposed modifications to [ITU-T X.672]

Based on previous clauses, this clause explores the potential work and discussion worthwhile in ITU-T Q11/17. The work is joint with ISO/IEC JTC 1/SC 6/WG 10.

A new version of [ITU-T X.672] is required to solve the ORS issues according to this Technical Report:

– Solve the performance issue and missing OID subtree issue in [ITU-T X.672] discussed in clause 6 without specifying two different systems;
– the changes and emphasis on management and administration of ORS zones according to the solution proposed in clause 8.2.2;

– provide implementation guidance of local cache according to solutions proposed in clauses 8.1.2, 8.1.3 and 8.1.4;
– provide operational guidance in a new version of [ITU-T X.672] according to clause 9;
– add a section to introduce changes and compatibility of the new version of [ITU-T X.672].

11.2 Proposed modifications to [ISO/IEC 29168-2]

Based on previous clauses, this clause lists the potential work and discussion worthwhile in ISO/IEC JTC 1/SC 6/WG 10.

According to clause 9, a new version of [ISO/IEC 29168-2] should add the role of secondary operational agency who operates the secondary DNS server for `oid-res.org`.

Bibliography

[b-ITU-T X.675] Recommendation ITU-T X.675 (2015), *OID-based resolution framework for heterogeneous identifiers and locators*.

[b-ITU-T X.676] Recommendation ITU-T X.676 (2018), *Object identifier-based resolution framework for IoT grouped services*.

[b-IETF RFC 1035] IETF RFC 1035 (1987), STD 13, *Domain names – implementation and specification*.
<https://www.rfc-editor.org/info/rfc1035>

[b-IETF RFC 2915] IETF RFC 2915 (2000), *The Naming Authority Pointer (NAPTR) DNS Resource Record*.
<https://www.ietf.org/rfc/rfc2915.txt>

[b-IETF RFC 4033] IETF RFC 4033 (2005), *DNS Security Introduction and Requirements*.
<https://www.rfc-editor.org/info/rfc4033>

[b-IETF RFC 5074] IETF RFC 5074 (2007), *DNSSEC Lookaside Validation (DLV)*.
<https://www.rfc-editor.org/info/rfc5074>

[b-IETF RFC 5936] IETF RFC 5936 (2010), *DNS Zone Transfer Protocol (AXFR)*.
<https://www.rfc-editor.org/info/rfc5936>

[b-IETF RFC 6116] IETF RFC 6116 (2011), *The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)*.
<https://www.rfc-editor.org/info/rfc6116>

[b-IETF RFC 7816] IETF RFC 7816 (2016), *DNS Query Name Minimisation to Improve Privacy*.
<https://www.rfc-editor.org/info/rfc7816>

[b-IETF RFC 8499] IETF RFC 8499, BCP 219 (2019), *DNS Terminology*.
<https://www.rfc-editor.org/info/rfc8499>

Annex A

Example of ORS zone supporting missing OID nodes

Figure A.1 shows an example of a zone file configuration to support OID `1.2.156.3001.3851`. This OID is missing because `1.2.156.3001` is not ORS-supported.

NOTE – In the diagram, `www.anydomain.com` is used for the URL. This is only for illustrative purpose and any URL can be used.

Figure A.1 – Example of a zone file configuration to support missing OID `1.2.156.3001.3851`