Based on the **errors.py** file in the DNSViz GitHub repository, I have extracted the following types of DNS issues that can be detected:

1. **FORMERR**: Format error - the server failed to understand the query.
2. **SERVFAIL**: Server failure - the server encountered an error while processing the query.
3. **NXDOMAIN**: Non-existent domain - the domain does not exist.
4. **NOTIMP**: Not implemented - the server does not support the requested query type.
5. **REFUSED**: Query refused - the server refuses to process the query.
6. **YXDOMAIN**: Name exists when it should not.
7. **YXRRSET**: RRset exists when it should not.
8. **NXRRSET**: RRset does not exist when it should.
9. **NOTAUTH**: Server is not authoritative for the zone.
10. **NOTZONE**: Name is not within the zone of authority.
11. **BADVERS**: Bad OPT version.
12. **BADSIG**: Bad signature - the signature is invalid.
13. **BADKEY**: Bad key - the key is invalid.
14. **BADTIME**: Bad time - the signature's time is invalid.
15. **BADMODE**: Bad mode - the mode is invalid.
16. **BADNAME**: Bad name - the name is invalid.
17. **BADALG**: Bad algorithm - the algorithm is invalid.
18. **BADTRUNC**: Bad truncation - the message is truncated.

These issues are related to various aspects of DNS, such as server errors, query errors, and security concerns. By analyzing the output of DNSViz, you can identify and address these potential issues in your DNS configuration.

Based on the **offline.py** file in the DNSViz GitHub repository, I have identified the following types of DNS issues that can be detected:

1. **DNSKEY**: Issues related to DNSKEY records, which are used for DNSSEC (DNS Security Extensions).
2. **DS**: Issues related to DS (Delegation Signer) records, which are used for DNSSEC.
3. **NSEC**: Issues related to NSEC (Next Secure) records, which are used for DNSSEC.
4. **NSEC3**: Issues related to NSEC3 records, which are an alternative to NSEC records in DNSSEC.
5. **NSEC3PARAM**: Issues related to NSEC3PARAM records, which are used to specify NSEC3 parameters.
6. **RRSIG**: Issues related to RRSIG (Resource Record Signature) records, which are used for DNSSEC.
7. **CDS**: Issues related to CDS (Child DS) records, which are used for DNSSEC key rollover.
8. **CDNSKEY**: Issues related to CDNSKEY (Child DNSKEY) records, which are used for DNSSEC key rollover.
9. **DLV**: Issues related to DLV (DNSSEC Lookaside Validation) records, which are an alternative trust anchor for DNSSEC.
10. **TLSA**: Issues related to TLSA (Transport Layer Security Authentication) records, which are used for DANE (DNS-based Authentication of Named Entities).
11. **SMIMEA**: Issues related to SMIMEA (S/MIME Certificate Association) records, which are used for DANE.
12. **SSHFP**: Issues related to SSHFP (SSH Public Key Fingerprint) records, which are used for secure shell (SSH) key fingerprints.
13. **IPSECKEY**: Issues related to IPSECKEY (IPsec Key) records, which are used for IPsec keying material.
14. **OPENPGPKEY**: Issues related to OPENPGPKEY (OpenPGP Key) records, which are used for OpenPGP keys.

These issues are mainly related to DNSSEC, DANE, and other DNS-related security extensions. By analyzing the output of DNSViz, you can identify and address these potential issues in your DNS configuration.

Based on the **online.py** file in the DNSViz GitHub repository, I have identified the following types of DNS issues that can be detected:

1. **NO\_ANSWERS**: When no answers are provided by authoritative servers for a specific query.
2. **TRUNCATED**: When the response to a query is truncated due to the size of the response exceeding the maximum allowed by the protocol.
3. **LAME**: When an authoritative server for a zone is not providing authoritative answers for that zone.
4. **EDNS\_NO\_SUPPORT**: When an authoritative server does not support EDNS (Extension Mechanisms for DNS).
5. **EDNS\_VERSION**: When an authoritative server does not support the specified EDNS version.
6. **EDNS\_FLAG**: When an authoritative server does not properly handle the specified EDNS flags.
7. **EDNS\_OPT**: When an authoritative server does not properly handle the specified EDNS options.
8. **UNKNOWN\_OPTION**: When an authoritative server does not recognize the specified EDNS options.
9. **NO\_TCP**: When an authoritative server does not support DNS queries over TCP.
10. **NO\_COOKIE\_OPT**: When an authoritative server does not support DNS cookies.
11. **COOKIE\_OPT\_MISMATCH**: When an authoritative server responds with an incorrect DNS cookie.
12. **COOKIE\_NO\_SERVER\_COOKIE**: When an authoritative server does not include a server cookie in its response.

These issues are mainly related to the DNS query/response process, support for different DNS transport protocols, and handling of various DNS extensions. By analyzing the output of DNSViz, you can identify and address these potential issues in your DNS configuration.

Based on the **status.py** file in the DNSViz GitHub repository, I have extracted the following types of DNS issues that can be detected:

1. **NO\_ANSWERS**: No answers received for the query.
2. **INCONSISTENT**: Inconsistent data received from different servers.
3. **SERVFAIL**: Server failure during the query process.
4. **REFERRAL\_ERROR**: Incorrect or unexpected referral received.
5. **NO\_NS\_ADDRESSES**: No address records for nameservers.
6. **LAME\_DELEGATION**: Lame delegation detected.
7. **INVALID**: Invalid data received.
8. **INSECURE\_DELEGATION**: Insecure delegation detected.
9. **BOGUS\_DELEGATION**: Bogus delegation detected.
10. **INCOMPLETE**: Incomplete DNS data received.
11. **BOGUS**: Bogus data detected.
12. **INSECURE**: Insecure data detected.
13. **NON\_EXISTENT**: Non-existent data detected.
14. **INDIRECT**: Indirect data detected.
15. **INDETERMINATE**: Indeterminate data detected.
16. **EXPIRED**: Expired data detected.
17. **PREMATURE**: Premature data detected.
18. **ALGORITHM\_IGNORED**: Algorithm ignored during the process.
19. **KEY\_IGNORED**: Key ignored during the process.
20. **SIGNATURE\_ERROR**: Error related to DNSSEC signatures.
21. **INDETERMINATE\_NO\_DS**: Indeterminate data because no DS records were found.
22. **INDETERMINATE\_MATCH\_PRE\_REVOKE**: Indeterminate data because a pre-revoke match was found.
23. **INVALID\_SIG**: Invalid signature detected.
24. **INVALID\_SIG\_EXPIRED**: Invalid signature detected due to expiration.
25. **INVALID\_SIG\_PREMATURE**: Invalid signature detected due to being premature.
26. **INVALID\_SIG\_INCEPTION**: Invalid signature detected due to inception.
27. **INDETERMINATE\_SIG**: Indeterminate signature detected.
28. **INDETERMINATE\_SIG\_EXPIRED**: Indeterminate signature detected due to expiration.
29. **INDETERMINATE\_SIG\_PREMATURE**: Indeterminate signature detected due to being premature.
30. **INDETERMINATE\_SIG\_INCEPTION**: Indeterminate signature detected due to inception.
31. **DNSKEY\_NXDOMAIN**: No DNSKEY records found.
32. **DNSKEY\_NOAUTH**: No authoritative data for DNSKEY records.
33. **DNSKEY\_SERVFAIL**: Server failure while fetching DNSKEY records.
34. **RRSIG\_NXDOMAIN**: No RRSIG records found.
35. **RRSIG\_NOAUTH**: No authoritative data for RRSIG records.
36. **RRSIG\_SERVFAIL**: Server failure while fetching RRSIG records.

These issues are related to various aspects of DNS, such as data inconsistencies, server failures, delegation issues, security concerns, and more. By analyzing the output of DNSViz, you can identify and address these potential issues in your DNS configuration.