MLIS2021: Discussion about the Encrypted DNS hosted in Internal CPE

Pan Lanlan (潘蓝兰)

abbypan@gmail.com

Guangdong OPPO Mobile Telecommunications Corp. Ltd., China

2021.05

1. **Encrypted DNS Service**
   - Service Type
   - Service Provider
   - Server Address
   - Resolver Discovery
   - Resolver Validation
   - Special Scenario
2. **Encrypted DNS Service for Internal CPE**
   - Encrypted DNS Service Provider for Internal CPE
   - Our Proposal
3. **Conclusion**
   - Conclusion
   - Resources

Service Type

- DNS-over-TLS (DoT)
- DNS-over-HTTPS (DoH)
- DNSCurve

Service Provider

- Public DNS
- ISP DNS
- Internal CPE DNS

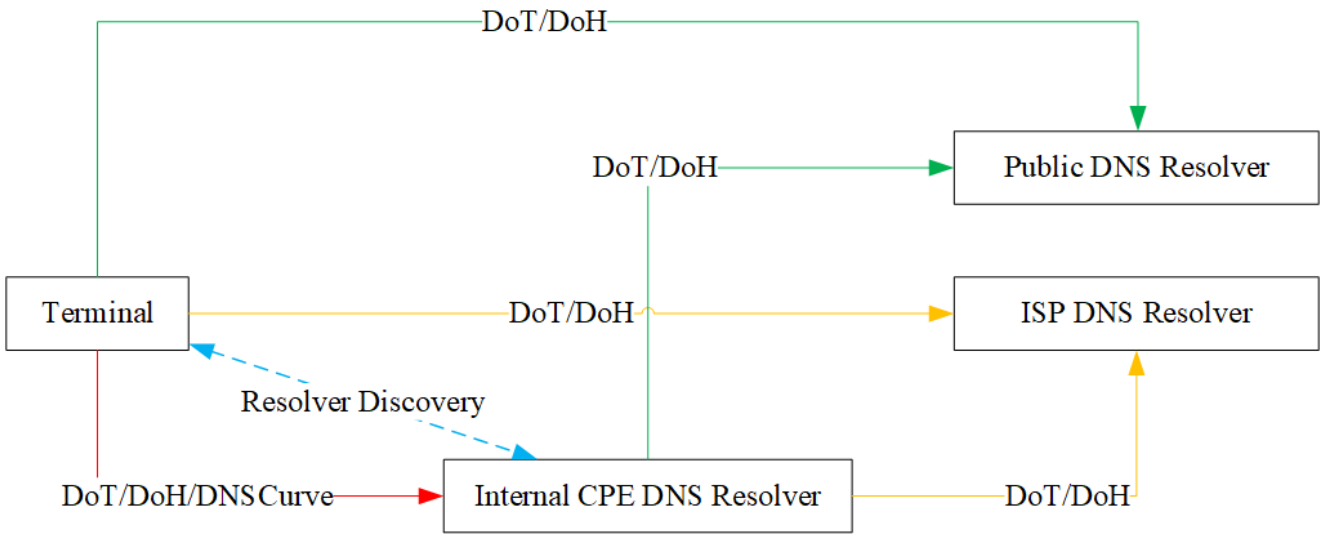


Fig: Service Provider

Server Address

- Authentication Domain Name(ADN)
- Public IP Address
- Private IP Address

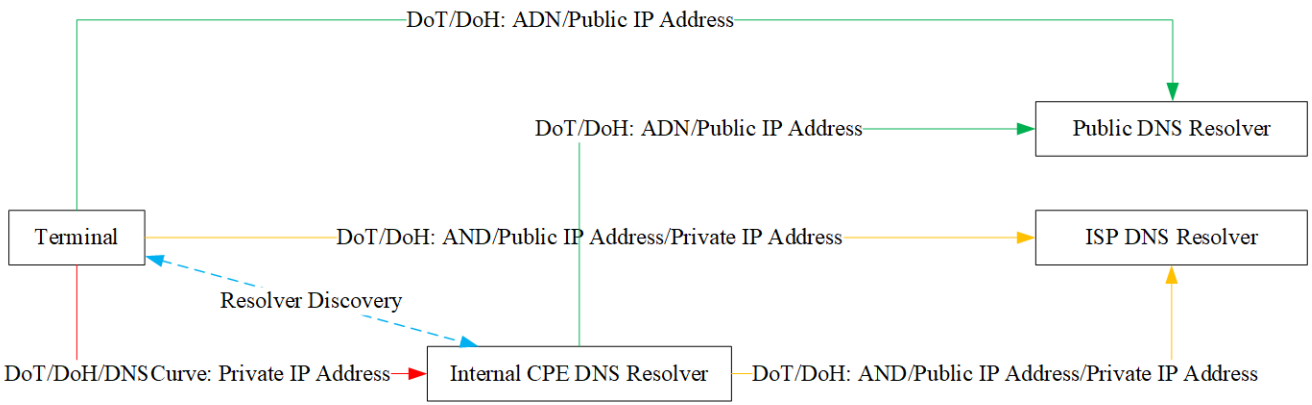


Fig: Server Address

Resolver Discovery

- Discovery of Network Designated Resolvers(DNR)
  - DHCP
  - Router Advertisement(RA)
- Discovery of Designated Resolvers(DDR)
  - domain: SVCB record
  - resolver: SVCB record from dns://resolver.arpa
- Adaptive DNS Resolver Discovery
  - SVCB record
  - provisioning domain (PvD) file

Resolver Validation

- DNSSEC-signed SVCB record
- PvD file: well-known HTTPS URI based on a zone apex
- TLS certificate: confirm of domain name ownership
  - certificate with trusted certificate chain
  - self-signed certificate

Special Scenario

- IoT secure bootstrap
  - use PAKE scheme to authenticate the EST server, and fetch the certificate
- BYOD
  - VPN tunnel

Encrypted DNS Service Provider for Internal CPE: Public DNS

- Server Address: ADN/Public IP Address
- Service Type: DoT/DoH
- Resolver Discovery: DHCP/RA/SVCB resolver.arpa
- Resolver Validation: DNSSEC/TLS certificate

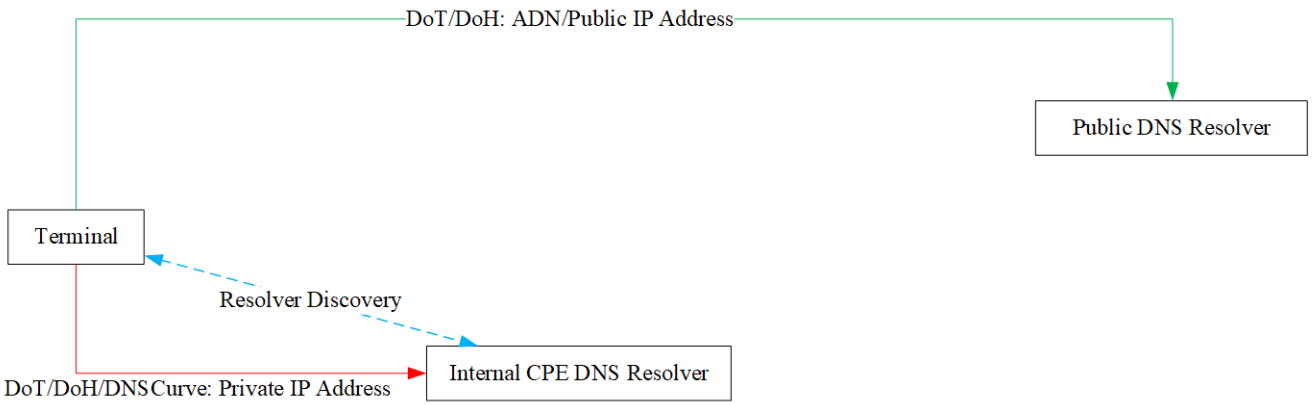


Fig: Public DNS

Encrypted DNS Service Provider for Internal CPE: ISP DNS

- Server Address: ADN/Public IP Address/Private IP Address
- Service Type: DoT/DoH
- Resolver Discovery: DHCP/RA/SVCB resolver.arpa
- Resolver Validation: DNSSEC/TLS certificate

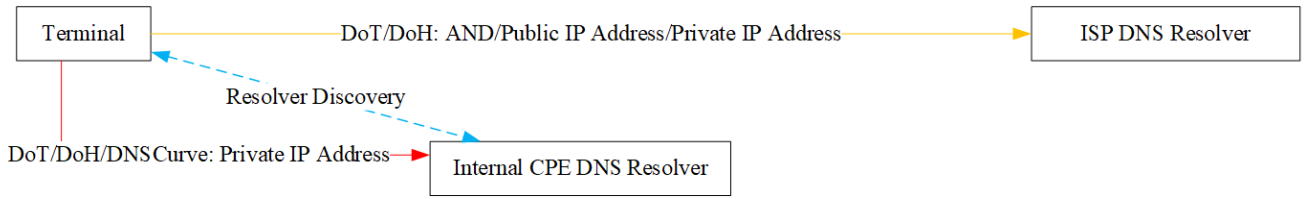


Fig: ISP DNS

the Encrypted DNS hosted in Internal CPE

- Server Address: Private IP Address
- Service Type: DoT/DoH
- Resolver Discovery: DHCP/RA/SVCB resolver.arpa
- Resolver Validation: TLS certificate

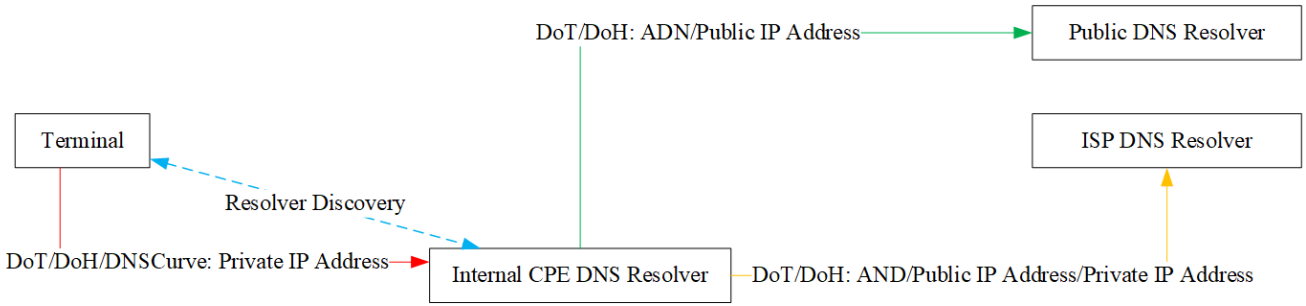


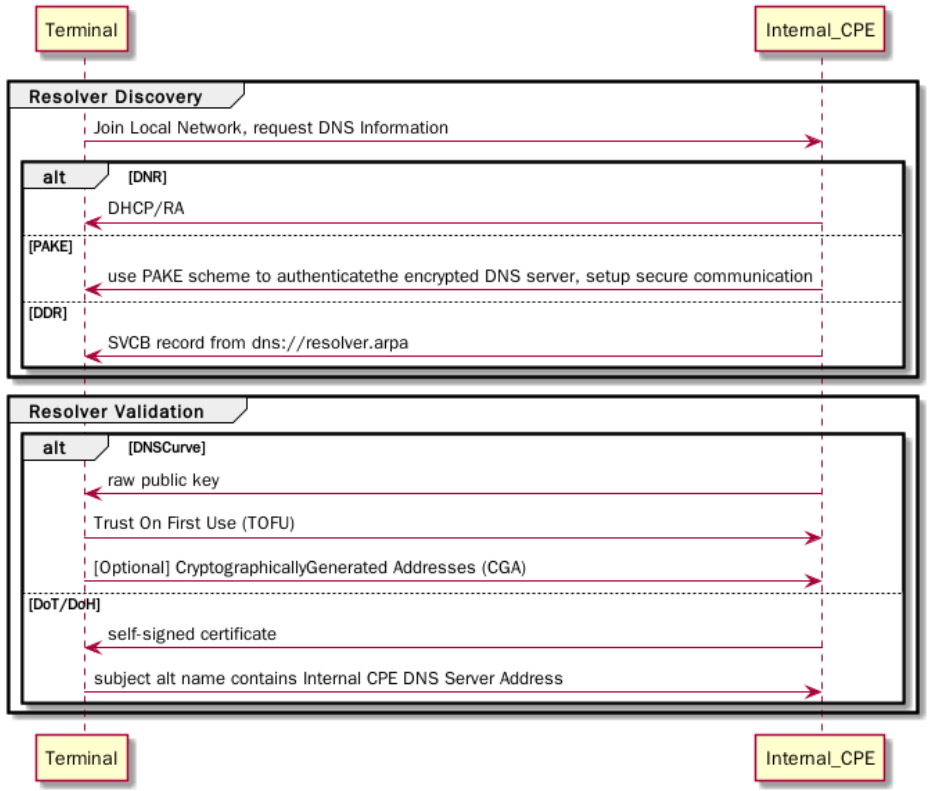
Fig: CPE DNS

Resource Constrained IoT Device

- Limited CPU/Memory/Battery
- Defense against Mirai DDoS attack
- DNS packet at local network without DNSSEC validation
- MDNS/DNSSD at local network probably without authentication

the Encrypted DNS hosted in Internal CPE: Lightweight

Make IoT device use the Encrypted DNS hosted in Internal CPE will be helpful to make access control on DNS query, and design filter policy against Mirai DDoS attack.



Conclusion

It is important to enhance security and privacy on local network communication.
We should design an local network DNS ecosystem, which is secure and affordable for resource constrained device.

Resources

- Discovery of Designated Resolvers
  https://github.com/ietf-wg-add/draft-ietf-add-ddr
- Discovery of Network provided Resolvers
  https://github.com/ietf-wg-add/draft-ietf-add-dnr
- DNS-over-HTTPS and DNS-over-TLS Server Deployment Considerations for Enterprise Networks
  https://datatracker.ietf.org/doc/draft-reddy-add-enterprise/
- Adaptive DNS Resolver Discovery
  https://tools.ietf.org/html/draft-pauly-add-resolver-discovery-01
- DNSCurve https://dnscurve.org/
- Cryptographically Generated Address
  https://en.wikipedia.org/wiki/Cryptographically_Generated_Address