中国移动
China Mobile

Dots server deployment consideration

draft-chen-dots-server-hierarchical-deployment-00

Meiling Chen, Li Su, Jin Peng

China Mobile Research Institute

July 2019

There are several deployment requirements mentioned in the current drafts, When we wanted to apply DOTS, we had the problem of how do we implement these requirements.

Related drafts and contents about deployment

ietf-dots-architecture :

This does not necessarily imply that the attack target and the DOTS client have to be co-located in the same administrative domain, **but it is expected to be a common scenario.** Although **co-location of DOTS server and mitigator within the same domain is expected to be a common deployment model**, it is assumed that operators may require alternative models.

ietf-dots-server-discovery :

A key point in the deployment of DOTS is the ability of network operators to be able to onfigure DOTS clients with the correct DOTS server(s) information consistently.

ietf-dots-multihoming :

when conveying a mitigation request to protect the attack target, **the DOTS client among the DOTS servers available Must select a DOTS server whose network has assigned the prefixes from which target prefixes and target IP addresses are derived**. This implies that no appropriate DOTS server is found, the DOTS client must not send the mitigation request to any DOTS server.

To meet the deployment requirements, it is necessary to understand the capabilities of dots server

Related drafts and contents about dots server ability

draft-ietf-dots-signal-channel-35

Section 4.4.1：

target-prefix: **the DOTS server MUST validate that target prefixes are within the scope of the DOTS client domain.**

Section 10:

DOTS servers MUST verify that requesting DOTS clients are entitled to trigger actions on a given IP prefix. That is, only actions on IP resources that belong to the DOTS client' domain MUST be authorized by a DOTS server. **The exact mechanism for the DOTS servers to validate that the target prefixes are within the scope of the DOTS client domain is deployment-specific.**

draft-ietf-dots-signal-call-home-03

Section 3.3.1:

source-prefix: **In addition, the DOTS client MUST validate that attacker prefixes are within the scope of the DOTS server domain.**

But how to satiesfy the requirement, We need more thorough discussions about deployment and functionality, and discuss how to implement it?

Draft-chen-dots-server-hierarchical-deployment-00

Motivation: This is DOTS server deployment guidance for operators, We've written about our experience as an ISP, and we hope that other scenarios will contribute as well.

What kind of equipments can be mitigators?

● router，

● Special cleaning equipment ，

● Network security equipment

Dots server exist as a single network element? should depend on existing equipment?

Conditions that should be met to deploy dots server

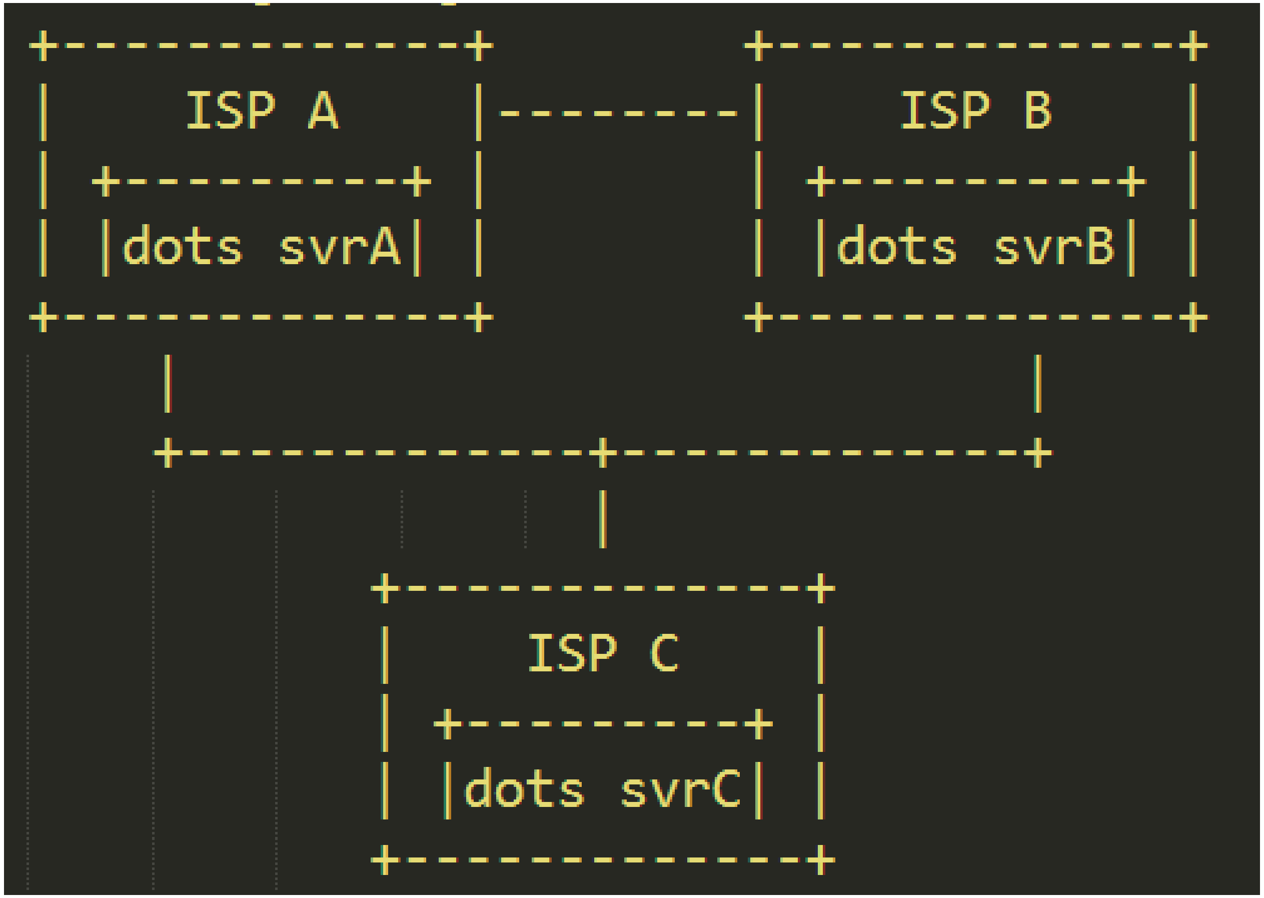
● DOTS server has to interconnected with mitigator , for most of the mitigators are in Intranet environments;

● DOTS server can go directly to the mitigator which had best go through without any other DOTS agents, such as gateway ;

● DOTS server has the permissions for scheduling and operations on mitigator ;

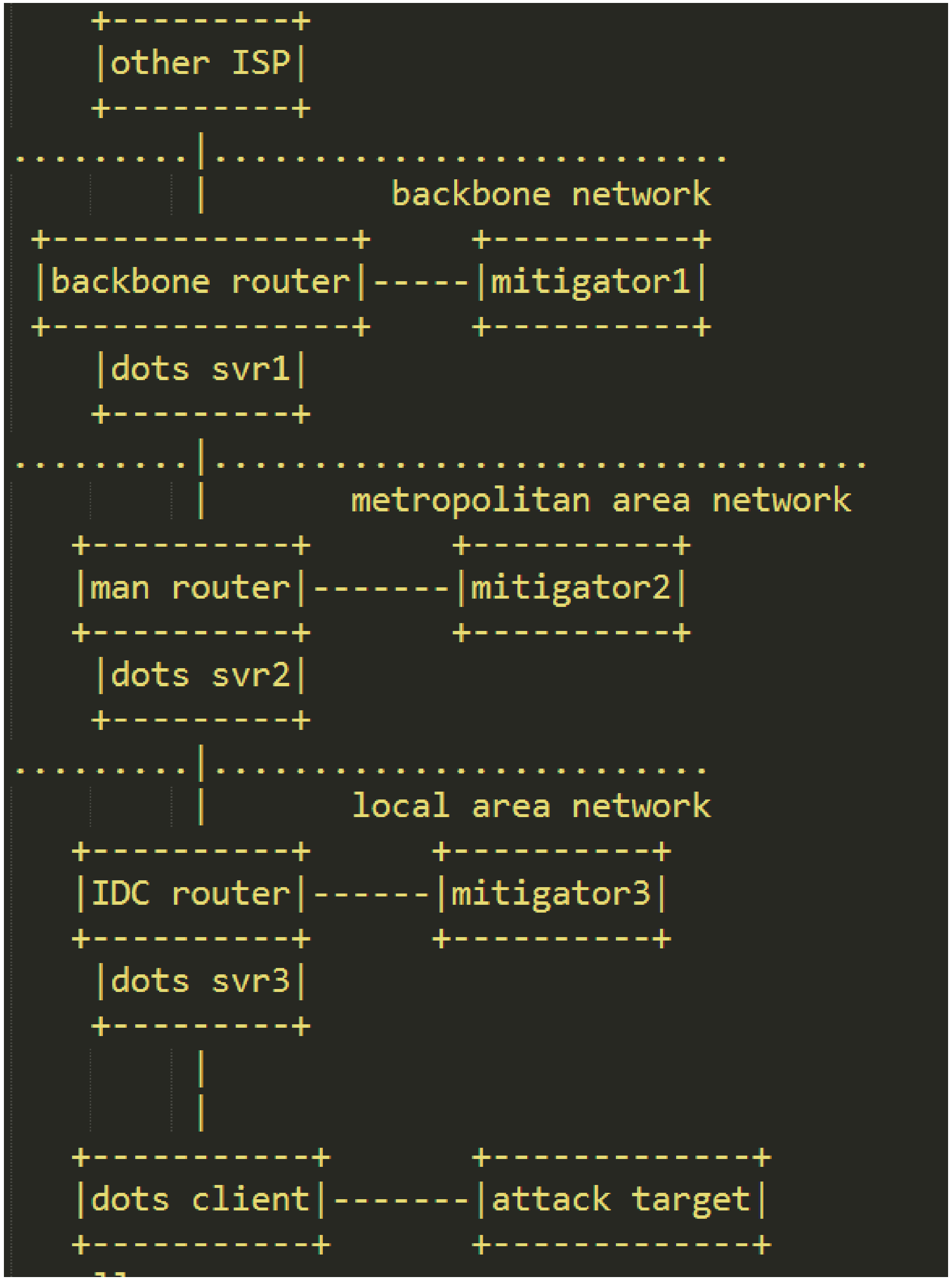
● DOTS server has the ability to know the address of attack target belong to which mitigator 。

Between ISPs



```
+-------------+        +-------------+
|    ISP A    |--------|    ISP B    |
| +---------+ |        | +---------+ |
| |dots svrA| |        | |dots svrB| |
+-------------+        +-------------+
    |                           |
    +-------------+-------------+
                  |
           +-------------+
           |    ISP C    |
           | +---------+ |
           | |dots svrC| |
           +-------------+
```

Inside an ISP



```
    +---------+
    |other ISP|
    +---------+
         |
.........|..........................
         |         backbone network
 +---------------+     +----------+
 |backbone router|-----|mitigator1|
 +---------------+     +----------+
    |dots svr1|
    +---------+
         |
.........|.................................
         |       metropolitan area network
   +----------+       +----------+
   |man router|-------|mitigator2|
   +----------+       +----------+
    |dots svr2|
    +---------+
         |
.........|.........................
         |       local area network
   +----------+      +----------+
   |IDC router|------|mitigator3|
   +----------+      +----------+
    |dots svr3|
    +---------+
         |
         |
   +-----------+       +-------------+
   |dots client|-------|attack target|
   +-----------+       +-------------+
```

Next steps:

1. Comments
2. Questions?