Trust Networking and Procedures for Autonomic Networking Update in -01

draft-choi-anima-trust-networking-01

November 5, 2018

IETF 103

Bankok

Taesang Choi, Taesoo Chung, ETRI
Junkyun Choi, Jaeseop Han, Woojik Chun, KAIST

Two main comments made in the 102th meeting

- Differences between Trust Autonomic Domain (TAD) and ANIMA security framework
- Implementation experience of TAD based ANIMA (architecture, protocols, etc.) as a use case

Update in draft-choi-anima-trust-networking-01

- Section 4. Differences between trust networking and ANIMA security framework is added.
- This section describes major differences between the proposed trust autonomic domain (TAD) and ANIMA security framework.
- The differences are explained based on a following set of criteria defined in the draft-carpenter-limited-domains-04:
- **domain as a whole, domain members, domain boundary, topology, technology, connection to the Internet, security/trust/privacy model, and operation**
- since our proposed domain and that of ANIMA are kinds of limited domains.

Differences between TAD and ANMIMA Security

Differences in terms of Limited Domain Taxonomy- **Domain as a whole**

- The domain in this document is defined as the networking region that shares common characteristics and also is distinguished from the rest of the network.
- Traditional layers cover its own regions implicitly; the physical layer spans the range covering electric signals. The data link covers the range connected by layer 2 bridges, and the network layer covers the whole devices connected by routers, and so on.
- Instead of implicit regions of the layers, a **domain** can be **defined as any region of the network which is distinguishable from the rest of the network**.
- It can be defined as a region covered by electric signal, a home network owned by a single user, a virtual private network overlaid on the Internet, a social network composed of members. Thus, it can be defined by any layer.

- **In the context of TAD,** the domain can be **defined by trust.**
- That means all members **within a TAD trust each other** so that the members can communicate with others **without any concern of security.**
- For this, **TAD needs to add an additional ASA - domain administrator.**
- Its main functionality is to **manage trust policies** including **allocating trust level** to domains and their members.
- Domain administrator can be **extended from the functionality of ANIMA MASA or** define **a new ASA.**
- The details of domain administrator is specified in Section 5 below.

Differences in terms of Limited Domain Taxonomy- **Individual Nodes (Domain members)**

- Since a domain shares common characteristics, any node within the domain must be able to communicate with other nodes in the domain.
- The node can be **host, networking devices, applications** depending on the characteristics of the domain.
- A node trying to be a new member of the domain must prove its functionalities to all or a designated member of the domain.
- Joining to a domain may be accomplished by simply plugging interfaces to the networking device or well-defined interactions enforced by domain administrator.
- The joining procedure may be implicit when a domain has fixed and permanent members, or explicit in case that a node can join or leave the domain.

- In the sense of **TAD,** a node is assumed **as a host that has communication functions required by the domain**.
- Since a TAD is defined under the intent of trust, **a node** should have **identifiable and authenticatable ID.**
- TAD utilizes a concept of self-certifying ID. The self-certifying ID can be newly defined. However, in the context of TDA as an application use case of ANIMA, **we can utilize IdevID as a self-certifiable ID** and
- preferably extend IdevID with public key information as an option to ensure the global uniqueness.

Differences in terms of Limited Domain Taxonomy- **Domain Boundary**

- Since a domain is a set of nodes that shares common characteristics, only nodes within a domain can communicate.
- **Special node** that belong multiple domains simultaneously, "**gateway**".
- The role of gateway is conveying interactions of one domain to other domains: **interpretation, filtering, transformation** etc.
- From outside of a domain, the **internals of the domain is hidden** and **the boundary of the domain composed of gateways are only exposed**.

- In the context of **TAD, all members of a TAD trust each other,** but cannot trust nodes outside of the domain.
- The only way for an internal node to communicate with external nodes is passing through a gateway of the domain.
- Once **the gateway** receives communication request from a node outside of the domain, it **authenticates the node and evaluates the trustworthiness of the node.** If the **external node is trustworthy and communication channel between gateway and the node is safe and reliable** enough for the domain trust level, the gateway accepts communication and injects the communication possibly with transformation.
- Unlike ANIMA which assumes IP based communications by every domains, TAD may allow any networking technology besides IP.
- Therefore, **a gateway is a mandatory component where the need for it is implicit in ANIMA due to the homogenous nature of networking technology used in a domain.**
- The details of domain gateway functionality is specified in Section 5 below.

Differences in terms of Limited Domain Taxonomy- **Topology**

- The communication can be done in either specific layer protocols or any common functionalities.
- For example, if domain is defined by local area network, the domain may use local IP addresses, link-local or site-local. For domains defined by virtual network overlaid on global Internet may use global IP addresses with filtering functions.
- Some special nodes may belong to multiple domains. In this case the range of the domains that involve the same nodes can be viewed as overlapped domains.
- The node belonging multiple domains should have multiple functionalities, one of each domain. Those functionalities should be separated.
- We can find similar situation in multi-homed IP host in the Internet, where the host has separate IP addresses, one for each IP address domain.
- **In the context of TAD, domains also have self-certifying ID as an ordinary node to become a member of another domain.**
- **The domain administrator must take a role of the required procedures of the parent domain such as trust evaluation, join and leave. Also the gateways must take necessary translation of the interactions when passing the domain boundary.**

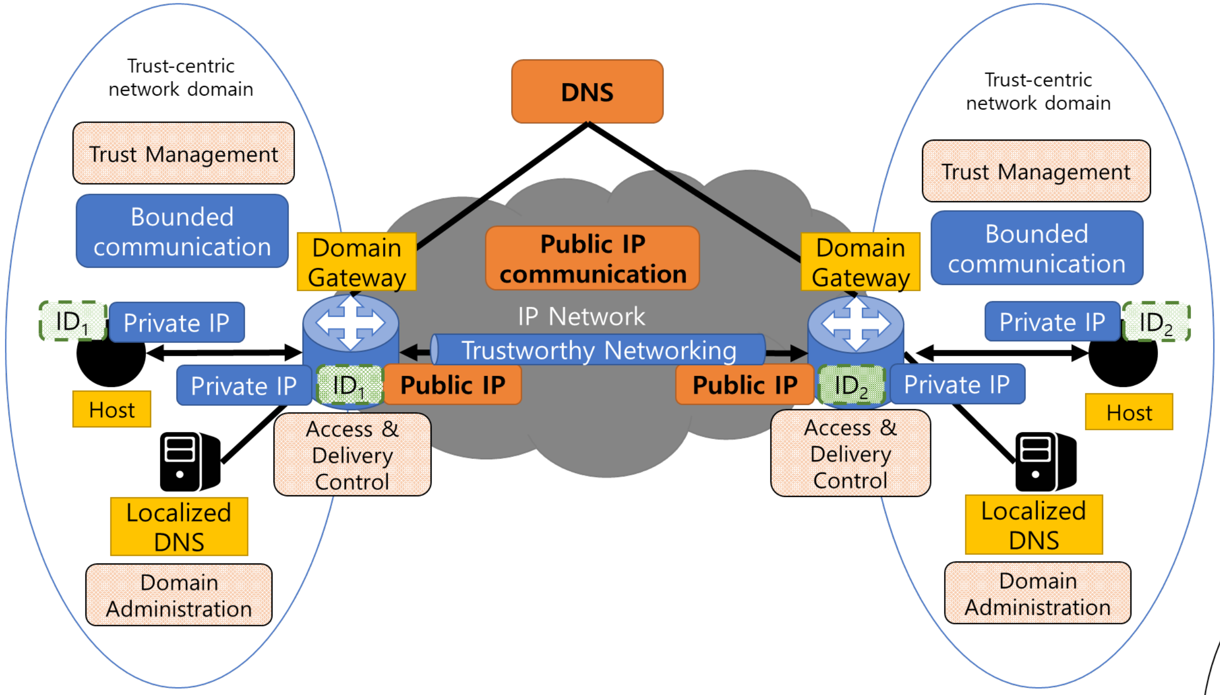
Differences in terms of Limited Domain Taxonomy- **Technology**

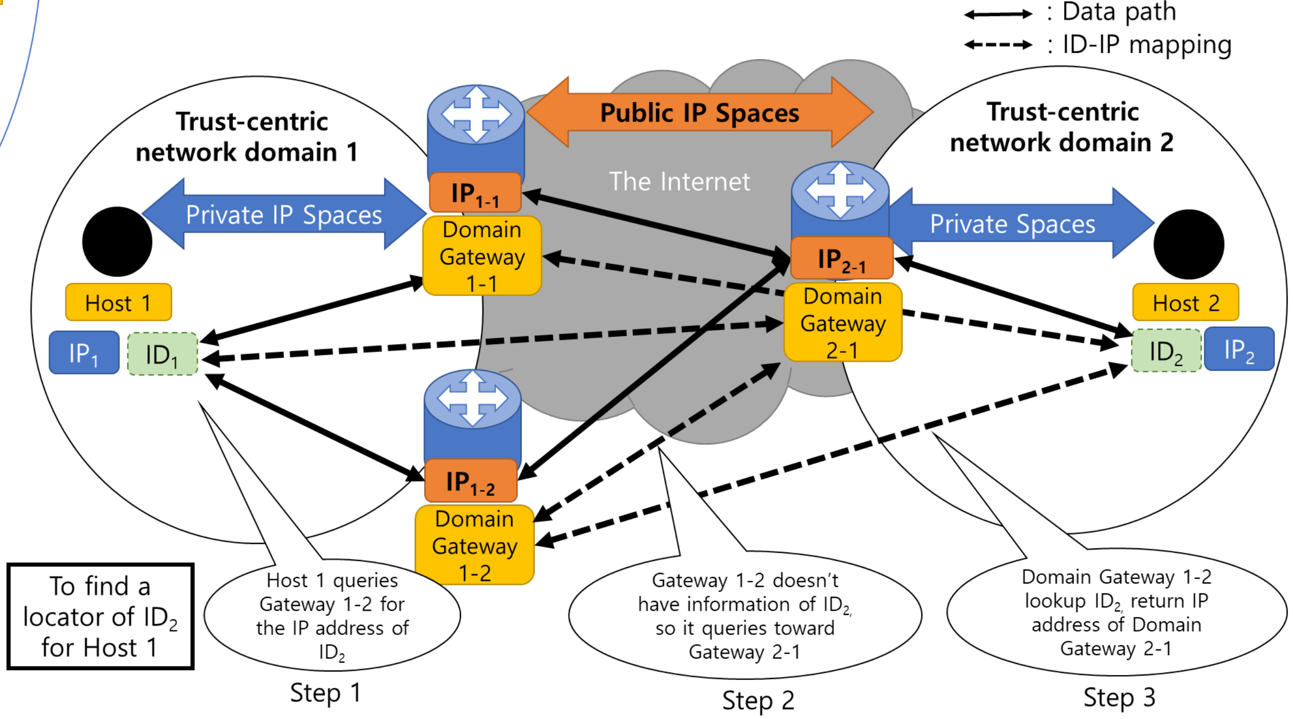
- In the context of TAD, **any technology is allowed for the domain** since a domain has its own mechanisms hidden from outside.
- Apart from the existing Internet using global IP addresses, each domain may use its own routing or forwarding mechanisms, such as Ethernet, MPLS, or Upper-Layer IDs.
- **Only requirement for inter-domain communication** is that the gateway must **aware of mechanisms for both domain and takes a role of translation**.
- Note that **each domain has a domain specific addressing scheme and identification** of nodes/domains **must be done by globally unique identifier**.
- With the global ID a node can join a domain or move from one domain to another. In this case a node acquires a domain specific address when joining the domain.

Differences in terms of Limited Domain Taxonomy- **Connection to the Internet**

- In the context of **TAD**, the existing Internet can be viewed as a huge domain with global coverage.
- **Nodes or domains with IP capability can join the global Internet domain as members**. Since the existing Internet has no notion of ID, let us assume the global Internet domain top-level domain where every domain can join.
- Each domain with its specific mechanism can join the global Internet domain permanently or intermittently.
- **The communication from one domain to another domain through the global Internet domain** is done **by the normal IP communication**.
- However, **the gateway of each domain must translate its internal communication mechanism to that of the corresponding IP address communications**.
- More specifically, **Inter-domain communication is done by the global ID and the ID is translated into domain-specific address when passing the domain boundary**.
- **This ID based communication may be encapsulated in IP packet** when traversing the global Internet domain.
- To allow this translation, **the ID to IP address mapping system must be provided**, where IP address is the gateway address of the domain that involves the node with the ID.

Differences in terms of Limited Domain Taxonomy- **Connection to the Internet**





To find a locator of ID$_2$ for Host 1

Host 1 queries Gateway 1-2 for the IP address of ID$_2$

Step 1

Gateway 1-2 doesn't have information of ID$_2$, so it queries toward Gateway 2-1

Step 2

Domain Gateway 1-2 lookup ID$_2$, return IP address of Domain Gateway 2-1

Step 3

Differences in terms of Limited Domain Taxonomy- **Security, Trust and Privacy Model**

- One of implication of a domain is secure protection of the domain internals from the rest of the network.
- That is members of a domain should be identified, authenticated, and authorized. According to domain’s policies, well-defined procedures must be enforced to a node to become a member of the domain.

- In **TAD** all members of the domain must have **the same or higher trust level** than the domain requires**.**
- That means, **whenever a new node tries to be a member of the domain or an external node tries to communicate with an internal node,** the domain administrator must authenticate and evaluate the node. **Only the node passing the evaluation procedure is allowed** to communicate**.**
- In this case **communication must be done via channels safe and reliable enough for the trust level.**
- In some cases where **the channel is not safe nor reliable**, the communicating nodes **must authenticate or encrypt the traffic.**
- **Note that whether the traffic is protected or not depends on the risk level of the channel and trust level of the domain.** Unlike the VPN that protects all channels in the same security protocols, channels for a domain are additionally **protected only when the risk level of a specific channel is higher than required.**

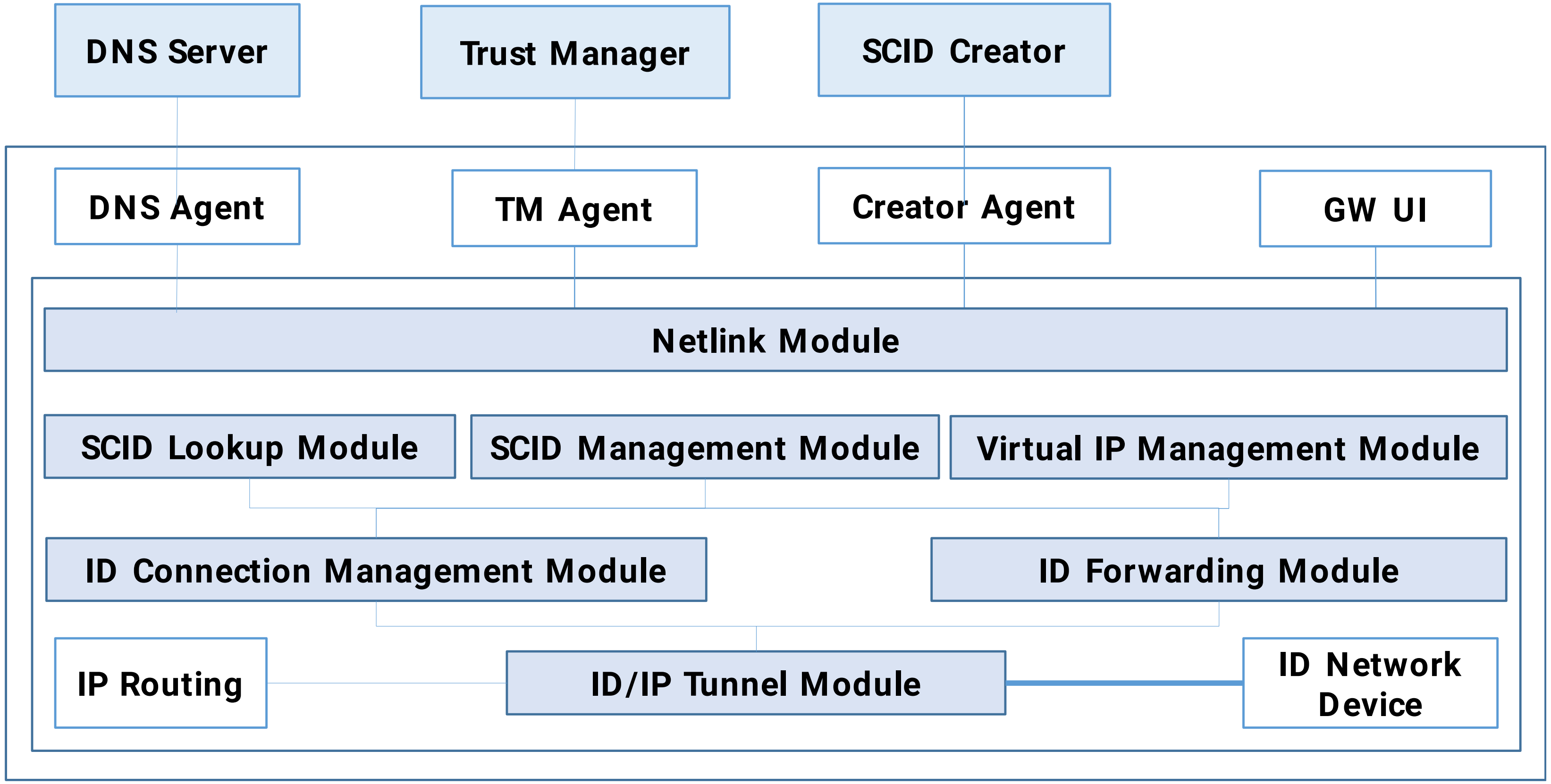
Differences in terms of Limited Domain Taxonomy- **Operations**

- In addition to trust relation between nodes within a domain, **the environment of the domain must be considered.**
- **Environment of a domain** includes factors affecting domain operation such as **communication channels among nodes, operation skills of domain administrator, reliability of devices, etc.** To be protected from the rest of networks, a domain should be securely protected from external attacks.
- Since communications within a **TAD** are carried out on **the mutual-trust basis**, **the domain administrator** should keep the domain trustworthy by **accepting only trusted members**, **monitoring traffic** to detect suspicious behavior, and **periodic auditing** the logs of domain members, and so on.

Introduction of TAD Implementation

TAD GATEWAY SYSTEM

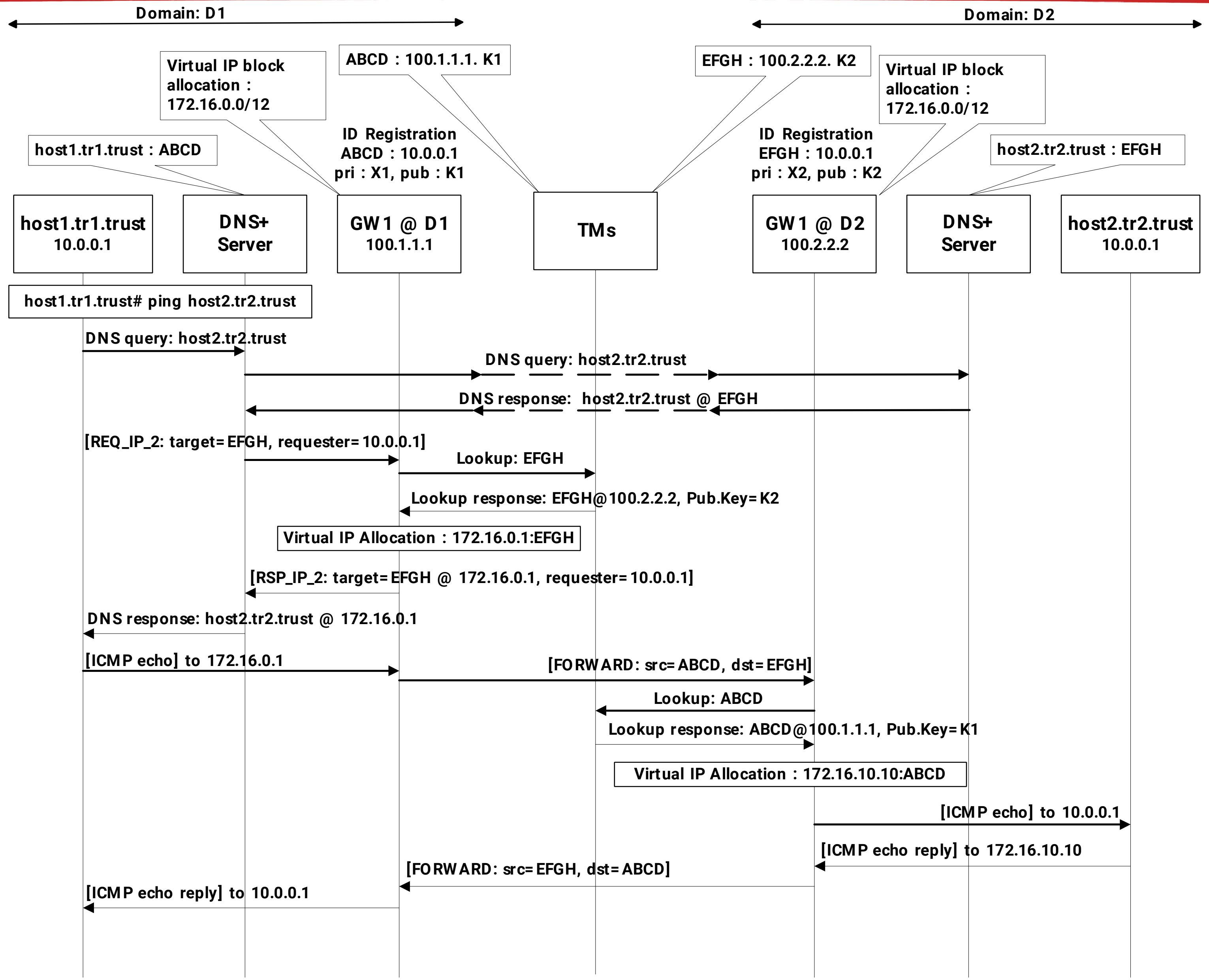
- The trust domain gateway system consists of 10 submodules.
- The trust domain gateway system has an external interface with a DNS server that is extended to provide a self-authentication identifier, a Trust Manager (TM) that manages the trust relationship, and a SCID creator that generates a SCID and delivers it to related systems.
- The relationship between external physical relations and each submodule inside the system is illustrated.



TAD GATEWAY SYSTEM

- Each submodule in the trust domain gateway system performs the following functions.
  - **Netlink module**: Perform communication function between application layer and kernel
  - **SCID Lookup module** : Perform the function to obtain information about host or upper / lower domain
  - **SCID Management module** : Perform the function of managing SCID information of Host or upper / lower domain
  - **ID Forwarding module**: Perform the message forwarding function on ID packet
  - **ID / IP Tunnel module**: Perform the function of transmitting ID packet through network
  - **DNS Agent module**: Pass the routing message from the extended DNS to the internal routing module
  - **TM Agent module**: Requests information about a domain or a host to Trust Manager and performs the function of transmitting information about the new domain
  - **ID Connection Management module** : Perform ID management for ID over IP entities
  - **Creator Agent** : Perform the function of receiving registration information for a new domain or host
  - **GW UI module**: Trust domain gateway environment management, domain configuration management, communication object information management functions, etc.

TAD COMMUNICATION PROCEDURE



Domain: D1

Domain: D2

Virtual IP block allocation : 172.16.0.0/12

ABCD : 100.1.1.1. K1

EFGH : 100.2.2.2. K2

Virtual IP block allocation : 172.16.0.0/12

host1.tr1.trust : ABCD

ID Registration
ABCD : 10.0.0.1
pri : X1, pub : K1

ID Registration
EFGH : 10.0.0.1
pri : X2, pub : K2

host2.tr2.trust : EFGH

host1.tr1.trust
10.0.0.1

DNS+
Server

GW1 @ D1
100.1.1.1

TMs

GW1 @ D2
100.2.2.2

DNS+
Server

host2.tr2.trust
10.0.0.1

host1.tr1.trust# ping host2.tr2.trust

DNS query: host2.tr2.trust

DNS query: host2.tr2.trust

DNS response: host2.tr2.trust @ EFGH

[REQ_IP_2: target=EFGH, requester=10.0.0.1]

Lookup: EFGH

Lookup response: EFGH@100.2.2.2, Pub.Key=K2

Virtual IP Allocation : 172.16.0.1:EFGH

[RSP_IP_2: target=EFGH @ 172.16.0.1, requester=10.0.0.1]

DNS response: host2.tr2.trust @ 172.16.0.1

[ICMP echo] to 172.16.0.1

[FORWARD: src=ABCD, dst=EFGH]

Lookup: ABCD

Lookup response: ABCD@100.1.1.1, Pub.Key=K1

Virtual IP Allocation : 172.16.10.10:ABCD

[ICMP echo] to 10.0.0.1

[ICMP echo reply] to 172.16.10.10

[FORWARD: src=EFGH, dst=ABCD]

[ICMP echo reply] to 10.0.0.1

TAD COMMUNICATION PROCEDURE

1. The source host1 requests the IP address of the destination host2 from the DNS server extended with the DNS query message.
2. The extended DNS server requests information about the destination host2 (destination GW2 address, SCID for the destination host) to the relative DNS server through DNS related information.
3. The source host1 and the destination host2 respectively register in the domain before communication.
4. When the host is registered, the IP address, Name, SCID, Public Key, and Private Key of the host are stored in the trust object table of the trusted domain gateway.
5. The source host1 requests to the extended DNS + server on the destination IP Host 2 to the DNS query message.
6. The extended DNS + server requests information about the destination host2 (destination GW2 address, SCID for the destination host) to the relative DNS + server through DNS related information.
7. GW1 asks TM for relevant information about host2. TM responds to GW1 with information about host2. GW1 forwards the received information to the DNS + server, creates a virtual IP, and creates a trust object table for host2.
8. The DNS + server that receives the response message from GW1 sends DNS response to host1.
9. The message of host1 whose routing is completed is forwarded from GW1 to GW2.
10. Upon receiving the forwarded message, GW2 requests the TM to lookup the source host1 for a response.
11. TM inquires registration information and responds with GW2 information about host1.
12. GW2 received the response transmits the lookup results to their DNS+ servers, and allocates the virtual IP.
13. Then, the message delivered from the trusted host1 is determined to be the IP address of the destination host, and the message is transmitted to the host2.
14. Host2 sends a response message after receiving the message.
15. GW2 forwards the response message of host2 to GW1, and GW1 forwards it to host1.

TAD - Test-bed

Five trust domains consisting of

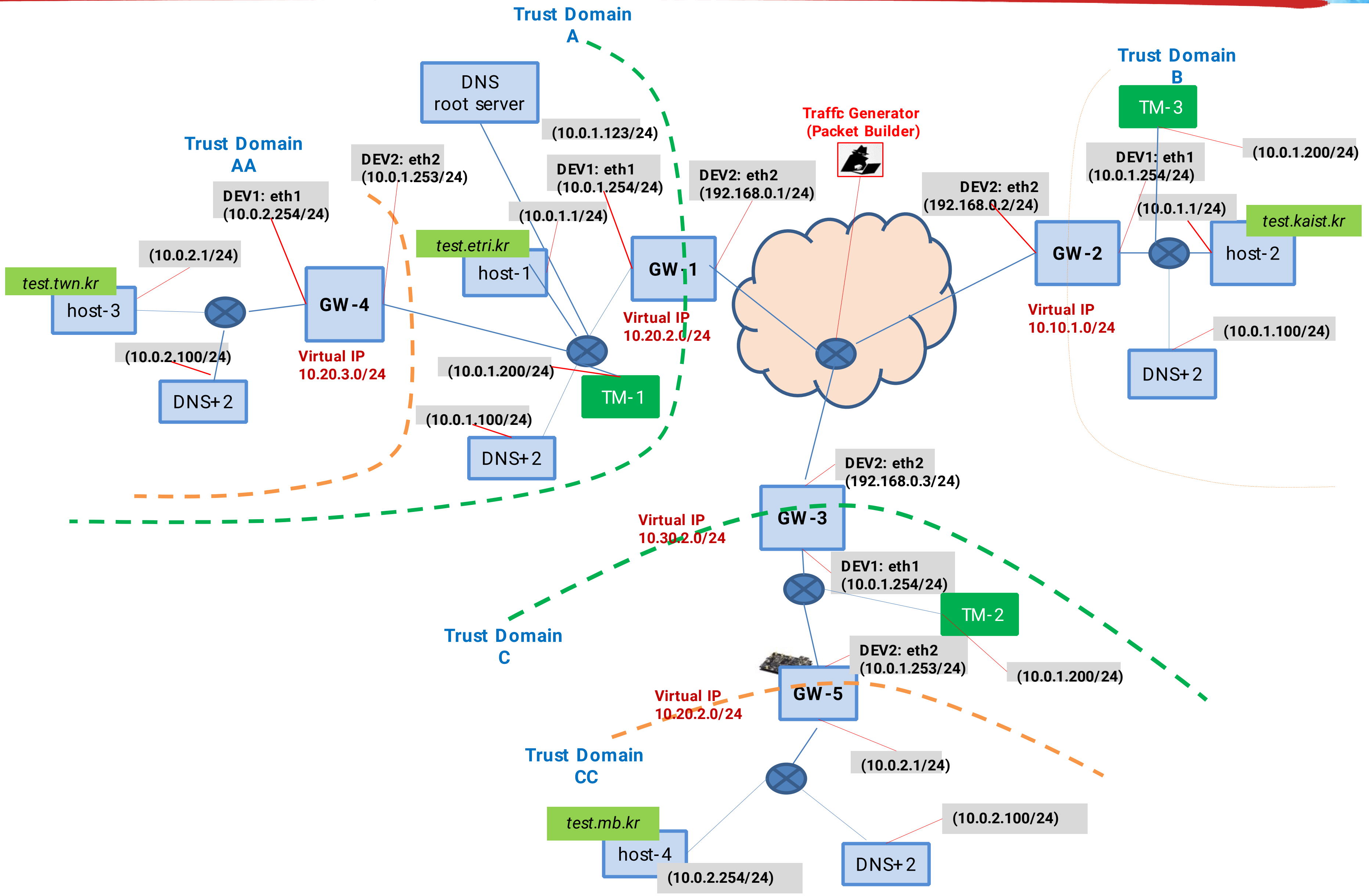
1 trust domain gateway,

1 host,

1 DNS + server, and

1 trust manager

per trust domain



Next Steps

- Solicit for further comments and feedbacks
- Update the document and prepare another version
- Wish that this topic will be in the scope of re-chartering?

Q&A

- choits@etri.re.kr