ANIMA
Internet Draft
Intended status: Standards Track
Expires: January 13, 2019

T.S.Choi
T.S.Jeong
ETRI
J.K.Choi
J.S.Han
KAIST

October 14, 2018

Trust networking and procedures for Autonomic Networking

draft-choi-anima-trust-networking-01

Abstract

This document describes trust networking as an application of autonomic networking. The objective of trustworthy autonomic networking is providing trust networking environment where all autonomic nodes can communicate without any security concern. It defines a trust networking domain and describes how to configure and maintain the trust networking domain. While communication within the trust networking domain is done with trust, the communication with external nodes should be done via a specific autonomic service agent (ASA) called "trust gateway". The trust gateway ASA performs trust evaluation of the external nodes and enforces domain specific policies to keep the domain trustworthy.

Status of This Memo

This Internet-Draft will expire on January 13, 2019

Copyright Notice

Table of Contents

1. Introduction 4
2. Background 4
2.1. Security Model and its Limitations 5
2.2. Trust Model and Trust Relations 6
2.3. Comparisons of Security and Trust Model 7
3. Trust Networking Framework 8
3.1. Defining Trust Networking Domain 9
3.2. Protecting Trust Networking Domain 9
3.3. Expanding Trust Networking Domain 10
3.4. Communicating with External Entities 11
4. Differences between trust networking and ANIMA security framework 12
4.1. Domain as a Whole 12
4.2. Individual Nodes (Domain members) 13
4.3. Domain Boundary..... 13
4.4. Topology 14
4.5. Technology 15
4.6. Connection to the Internet 15
4.7. Security, Trust and Privacy Model 16
4.8. Operations 16
5. Trust networking domain as an application of autonomic networking 17
5.1. Definition of a Trust networking domain 18
5.2. Configuration of Trust networking domain 19
5.3. Communication between Trusted Autonomic Nodes within a trust networking domain 20
5.4. Communication between trusted autonomic nodes and external nodes 20
6. Trust Networking in the Autonomic Networking Infrastructure 21
6.1. Identification of Trust networking domain and Trusted Autonomic Node 22
6.2. Discovery of Trust networking domain 23
6.3. Signaling Between Trusted Autonomic Nodes 23
6.4. Trust Evaluation 24
7. Procedures for trust networking 25
7.1. Building a trust networking domain 25
7.1.1. Domain initialization 25
7.1.2. Node registration 26
7.2. Evicting existing node from trust networking domain

..... 28

7.3. Terminating trust networking domain 28
7.4. Communication among trust networking domains 28
7.4.1. Trustworthy networking within a single trust networking domain 28
7.4.2. Trustworthy networking between trust networking domains 28
8. Security Considerations 30
9. IANA Considerations 31
10. Acknowledgements 31
11. Contributors 31
12. References 31
12.1. Normative References 31
12.2. Informative References 31

1. Introduction

The document describes the concept of trust networking as an application of Autonomic Networking Architecture. It defines a trust networking domain in compliance with reference model of autonomic networking. By definition of autonomic domain [rfc7575 Autonomic Networking Definitions and Design Goals] the trust networking domain is defined as a collection of autonomic nodes which trust other nodes in the same trust networking domain. That means, communications within the trust networking domain with sufficient trust level can be done without any further security concerns. For example, assume that a subnet properly protected from external threats and all nodes in the subnet are verified through trust evaluation procedures, then the communications within the subnet can be done with confidence that nodes do no harm to each other.

This document first defines a trust networking domain and then describes how to configure the trust networking domain and keep the domain trustworthy. This document also describes a trust networking framework that consists of interconnected trust networking domains. The framework guides how to define the trust networking domain, how to manage members of the domain, how to protect the domain from hostile external world, how to expand the domain, and how to handle communications with external entities. Finally this documents shows how to apply the trust networking framework to the existing IP based network with minor modifications

2. Background

One of the biggest problems in the current Internet is protecting information assets against divergent attacks. In the beginning of

the Internet, security was not considered to be an essential component of the network architecture but optional solutions such as IPSec were used instead. This section compares the security model of the traditional Internet and our proposed trust model.

2.1. Security Model and its Limitations

The security model of the current Internet is based on the assumption that all traffic coming from the Internet is suspicious. The lack of inherent security in IP protocol has led various attacks, such as attack on confidentiality by intercepting packets, integrity attack by modifying of the contents of packets, authentication attack by identity fabrication, and availability attack by interfering normal communications. In the context of untrusty Internet, each host should protect itself from potential risks of the hostile Internet. This protection usually take place at the final destination as seen in Figure 1. This model operates basically in reactive manner. That means, after receiving all arriving packets, threatening packets can be detected and removed. Detection of threatening packets are based on pre-defined rules extracted from previous attacks.

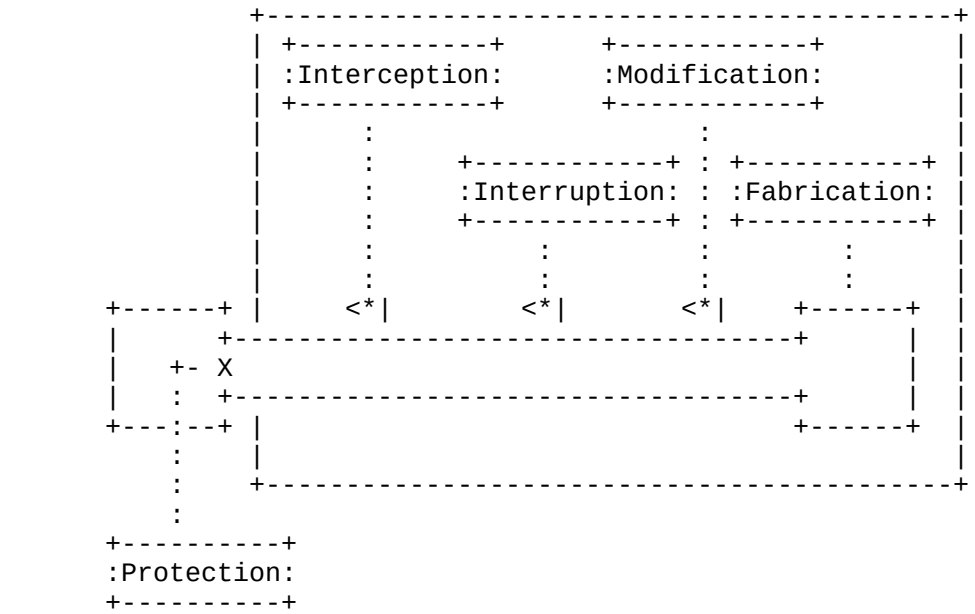


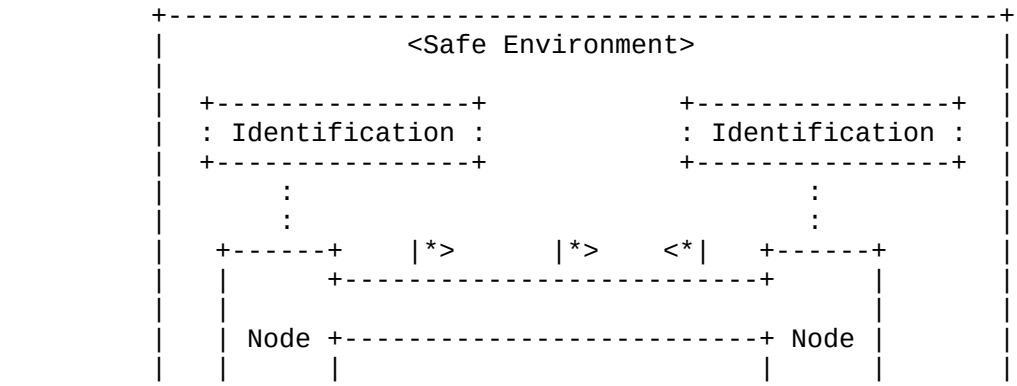
Figure 1. Security Model

The reactive operations of security model result in endless malicious cycle of attacks and defenses. Rules has to be upgraded for every newly discovered attacks and more complicate rules are required as more sophisticate attacks emerge. This model is fatal in the case of devices with limited or no processing power. Also stronger security makes the system weaker in defending DoS (Denial of Service) attacks.

2.2. Trust Model and Trust Relations

In contrast to the security model based on doubt, the trust model is based on the confidence that any entity in the domain is not harmful to other entities and the communication environment within the domain is safe enough. Instead of unlimited connectivity, the trust model restrict connectivity to the limited group of trusted entities. Of course, the limited connectivity can be extended by the domain expansion principle described in Section 3.3. Figure 2 illustrates the trust model, which needs 3 requirements: Identification, Trust Relation, and Safe Environment.

For identification purpose, the trust model uses self-certifying ID (SCID), which provides secure binding between ID and key of an entity. Many future Internet researches already use SCID for accountability or trusted path selection. The trust model assume that every entity has a public key and hash of the public key is defined as the ID of the entity. This ID can be used in validity check of claimed key against actual public key of the entity. The valid public key is basis of further identity verification. After identification the entity check trust relation with the peer entity so that only trusted entity is allowed to communicate.



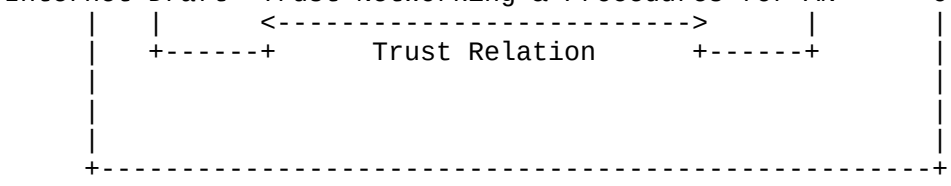


Figure 2. Trust Model

The trust relation used in the trust model is assumed to be reflexive, symmetric, and transitive. Reflexive means that entity A trust itself, denoting as AA. Symmetric relation assumes that two entities A and B satisfy AB and BA at the same time, denoting as AB. Transitive means that for three entities A, B, and C, if AB and BC then A C. If all entities in a given group satisfy all three characteristics, the group is declared as a trust equivalent class. We can easily guess the role of the trust model as formation of a trust equivalent class for the set of entities trusting each other.

The trust model should provide safe and reliable communication environment to entities without requiring additional security features on the entities. Thanks to the transitive trust relation, if an external entity is trusted by one member of the domain as a trust equivalence class, other members in that domain also can trust the external entity. By restricting the domain to trusted entities, the environment can be kept safe and reliable.

2.3. Comparisons of Security and Trust Model

The trust model is opposite in almost every aspect as shown in Table 1. First of all, the trust model is based on confidence that entities in a trust networking domain never do harm, while the security model is based on suspicion that adversaries attacks anytime. The relationship in trust model is binary in the sense that an entity trust another specific entity, but relationship in the security model is unary because the entity itself must protect regardless of other entities. With respect of rules, trust model keeps trusted IDs as a white list but security model keeps threatening entities as a black list. Thus, behavior of entities in the trust model is proactive while the security model acts in reactive manner. That leads the policy of the trust model is to prevent risk by communicating only with trusted entities, but policy of the security model monitors all communications to detect and remove threatening actions. The trust model provides mechanisms for

accepting entities or domains after verifying their trust, while the security model provides mechanisms for watching the traffic and blocking the threatening traffics. As the result, the network space of the trust model starts with a restricted space and incrementally glows as new entities or domains are accepted, while the network space of security model starts as an unrestricted and open space, but the space may be diminished by excluding misbehaving entities.

Table 1 Comparison of Trust and Security Model

	Trust Model	Security Model
based on	confidence	suspicion
relationship	binary	unary
rules	white list	black list
behavior	proactive	reactive
policy	prevention	detect and remove
mechanism	verify and accept	watch and block
network space	unrestricted and diminishing	rectricted and expanding

3. Trust Networking Framework

The purpose of the trustworthy communication framework is to provide safe and reliable environment to entities without requiring additional security features. For keeping the environment trustworthy, the domain accepts only eligible entities. However, this restriction seems contradict to global scalability that requires the domain being open to everyone. Our solution is the incremental strategy, where a domain starts from a small and restricted network space and gradually expands to a global scale

network space by accepting external entities or collaborating with other domains. This section discusses technical issues on the trustworthy communication framework.

3.1. Defining Trust Networking Domain

A primitive domain can be defined as the network space that is autonomous, isolated, and well protected from external attacks. For example, isolated home or enterprise network can be defined as a domain. If all hosts in the domain are disinfected and communication links are not exposed, the domain can be declared as a trust networking domain. The trust networking domain is not always a physical network space but sometime it can be formed by a logical group of users with mutual trust. In any case, the entities in the domain forms a trust equivalence class and communication with other entities in the domain is allowed without any protection.

To keep to domain trustworthy only qualified entities can be accepted as a member of the domain, and misbehaving entities have to be removed from the domain. For maintenance of a domain, the behavior of entities in the domain may be monitored, and if suspicious activities are discovered, the corresponding entity must be removed.

3.2. Protecting Trust Networking Domain

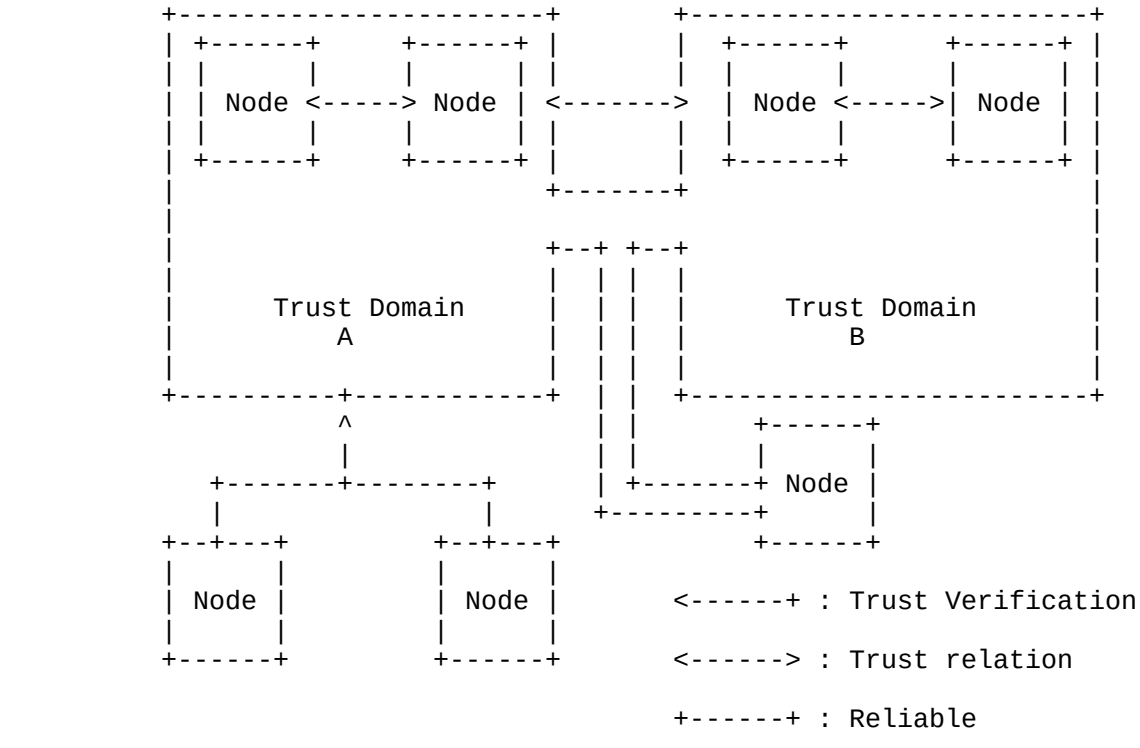
The domain representing an autonomous network space can take role of security unit as well as packet processing unit. The isolated domain from external world does not allow communication with external entities. For opening the domain to untrusty external world, well-defined interfaces are required to protect the domain. Let’s call this protected domain an "insulated trust networking domain". As an example of insulated trust networking domain, we can imagine the local area network with firewalls on all links to the external Internet. The local area network is not isolated but is insulated from attacks injected through the external links.

The proposed framework assumes that each domain has at least one gateway that performs security functions for the domain. The gateway identifies external entities, evaluate trust level, accepts or rejects the packets according to the trust levels of external entities. And also the gateway will forward only authorized and sterilized packets to peer domain for keeping its reputation or trust level. In the sense that gateways performs security functions on the behalf of the entities inside of the domain, the security of

entities is said to be delegated to gateways. This delegated security has great benefit in applying complex security functions to devices with a limited or no processing power.

3.3. Expanding Trust Networking Domain

If all communications are limited within a trust networking domain, the serious scalability arises with respect to global communication. Now, we have to consider expansion of trust networking domain, starting from a small trust networking domain to a global scale network. First, consider the situation that an entity outside of domain tries to communicate with an entity inside of the domain. For trustworthy communication across border of domain, the entity must be a member of the domain. The domain gateway performs well-defined procedure for checking identity and evaluating the trust level of the external entity, and then only qualified entities are allowed to communicate with entities in the domain. Also the link connecting the domain with external entities should be secure enough for the trust level. This is one way to expand a domain.



+------+ channel

Figure 3. Expansion of Trust Model

Expanding a domain by accepting new entities has limitation when reaching the maximum number of entities being managed by a single domain. The other solution is collaboration of domains. Suppose two domains trust each other and those are connected by reliable links, then entities within one domain can trust entities within another domain.

Figure 3 shows a trust networking domain with trusted entities and 3 ways how to expand the domain. First, new entities can join to the domain after passing trust verification. Second, a remote entity can join to the domain via reliable channel. And third, when two domains may have trust agreement and connected by reliable channel, all entities in one domain can exchange packets in the pre-agreed trust level.

3.4. Communicating with External Entities

As already seen, the communication inside of a domain requires no further security. However, communication with entities outside of the domain needs special care. Assume that all communication with external entities must take place at the special entity called a gateway, which enforce well-defined procedure communication for external entities. As explained in Section 3.3.2, an insulated trust networking domain has one or more gateways to perform trust verification for every packet injected to the domain.

When a packet arrives at the gateway of a domain, the gateway first check whether the source ID of the packet is in the trusted ID list. If exists, the packet is accepted. Otherwise, the gateway lookups the trusted domain list to find sending domain of the packet. If the sending domain is in the list, the packet can also be accepted and ID of the packet is saved in the trust ID list. This mean that the gateway believes the trusted sending domain not to send harmful packets. If ID of the packet is not in the trusted ID list nor the sending domain is in the trust networking domain list, then verification procedure for individual ID has to be performed. The procedure is somewhat similar to accepting new entities in the domain. The overall procedure of a gateway is shown in Figure 4.

4. Differences between trust networking and ANIMA security framework

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-03: 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.

4.1. Domain as a Whole

Networking is a very complex task and traditional way of handling the complexity is layering, where each layer takes a specific role and provides its services to the next higher later. This layering architecture decomposes the whole networking task functions vertically. However, the network in general spans physical or logical regions. Each region may have distinct features, such as different physical media, separate administration, and diverse networking requirement. The concept of 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 which performs a role of domain administrator. Its main functionality is to manage trust policies including allocating trust level to domains and their members. Domain administrator can extend the functionality of ANIMA MASA or define a new ASA for the purpose of the domain administration. The details of domain administrator is specified in Section 5 below.

4.2. Individual Nodes (Domain members)

As defined in the previous section, the domain covers a specific region of the network, to where a set of nodes belongs. Since a domain shares common characteristics, any node within the domain must be able to communicate with other nodes in the domain. The node as a member of a domain can be host, networking devices, applications depending on the characteristics of the domain. For keeping the same characteristics, 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.

4.3. Domain Boundary

Since a domain is a set of nodes that shares common characteristics, only nodes within a domain can communicate. In other words, a node within a domain cannot communicate with nodes outside of the domain. However, we can assume special nodes that belongs multiple domains simultaneously. Let’s call a node joining more than two domains a "gateway". A gateway node must be equipped with multiple functionalities, each for the joined domain. The role of gateway is conveying interactions of one domain to other domains. Of course, conveying interaction may include necessary functions such as 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. All interactions passing the boundary of a domain must performed by at least one of the gateways whose role is to enforce necessary gatewaying procedures.

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 networking technology used in a domain. The details of domain gateway functionality is specified in Section 5 below.

4.4. Topology

As defined in Section 4.1, a domain is a range of network where all members can communicate. 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.

As already explained in section 4.3, 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.

4.5. 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 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.

4.6. 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 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.

4.7. 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.

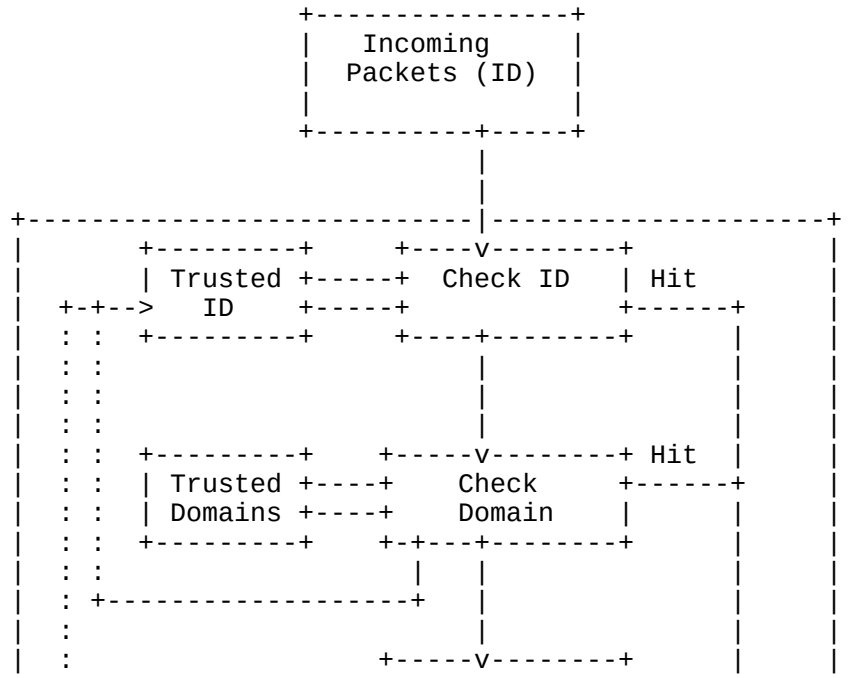
4.8. Operations

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.

5. Trust networking domain as an application of autonomic networking

This section defines what a trust networking domain is and describes how to configure the trust networking domain as an application of autonomic networking solutions. The autonomic nodes with trust networking domain will run with autonomic functions at Reference Model for Autonomic Networking. Autonomic networking infrastructure with trust management functions is capable to configure the trust networking domain. A set of autonomic nodes consists of a trust networking domain, which is configured, and managed by management plane. Within a trust networking domain, the full connectivity among autonomic nodes is securely and stably guaranteed. An autonomic node can easily communicate with other nodes at same trust networking domain. The trust level of autonomic nodes is calculated or assigned by trust evaluation function of management plane.
On the other hand, it is possible for autonomic nodes to communicate with different trust networking domains or non-autonomic networks via the trust gateway system, in which the traditional security or certificate mechanisms can be running.



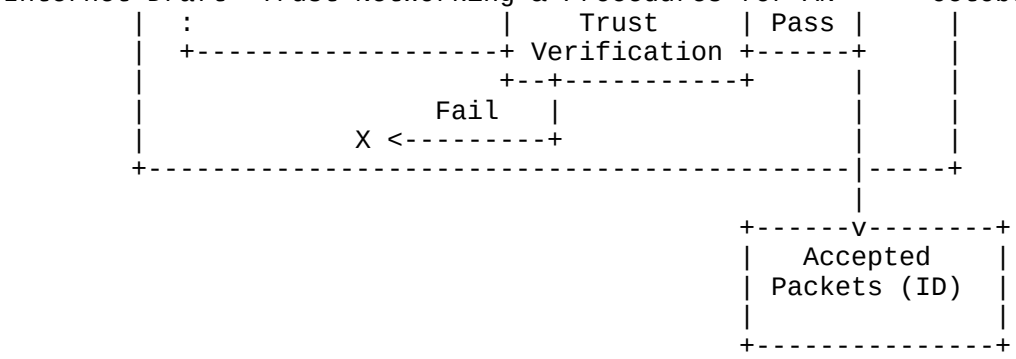


Figure 4. Packet Processing at the Gateway

5.1. Definition of a Trust networking domain

A trust networking domain is defined as a collection of autonomic nodes trusting each other. Since all nodes within a trust networking domain maintains certain trust level set by the domain, communications within the domain can be done without any further security concern. However, communications with external node require additional verification phase before the communications actually begin. The verification is performed at the border of the domain, where external nodes are checked if their trust level are sufficiently high for the domain. In the sense that the domain as a collection of node are protected from external world, it seems "zone defense" rather than "individual defense" of the traditional security scheme.

Figure 5 shows the high-level architectural view of trust networking domain. Autonomic nodes has the interface with management function. Trust management functions define the trusted autonomic nodes according to their trust level. They also define the trust networking domain by grouping or classifying autonomic nodes. At the same trust networking domain, an autonomic node directly communicates with each other. The control and management functions at the trust networking domain are defined at the interfaces between autonomic nodes and management plane.
There are trust gateway for an autonomic node to communicate with different trust networking domains or non-autonomic nodes since there is no direct communication path. Trust gateway is used to communicate autonomic nodes with different trust networking domains

or the non-autonomic nodes. An autonomic node can communicate remote autonomic nodes or non-autonomic nodes through trust gateway. In these cases, the traditional trust evaluation and/or certificate procedures can be applied at trust gateway. Trust evaluation procedure is running by management plane of autonomic networking.

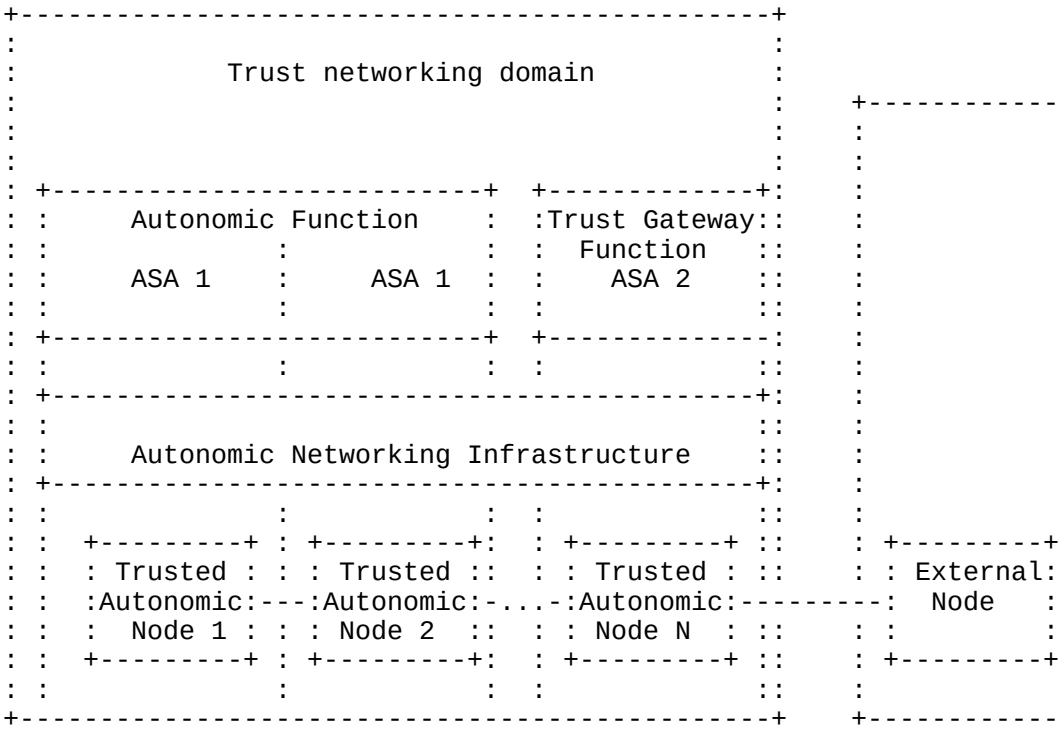


Figure 5. Trust networking domain at the Autonomic Networking

5.2. Configuration of Trust networking domain

A trust networking domain is consisted of a group of autonomic nodes. The network management plane communicates with a list of autonomic nodes to build the trust networking domain. The trust management information database which contains a list of autonomic nodes according to the trust level of each domain is built at the bootstrapping time or at the instance of request.

At the bootstrapping time, the management plane securely distributes the trust information of each domain to the corresponding autonomic nodes. The membership management is done by management plane when the autonomic nodes can be joined to or leaved from each trust networking domain.

At the instance that an autonomic node request to build a trust networking domain to the management plane, trust management function confirm to build a trust networking domain after completing the proper trust evaluation procedures.

If an autonomic node could not continue to be a member of the certain trust networking domain, it notify to management plane for leave. Similarly, if the trust management functions decide that an autonomic node is not relevant to stay in a certain trust networking domain, they notify the corresponding autonomic node for leave and update the trust management information database.

Within a trust networking domain, an autonomic node can communicate each other without any additional security and certificate procedure. In a case, an autonomic node may register multiple trust networking domains simultaneously.

5.3. Communication between Trusted Autonomic Nodes within a trust networking domain

At the same trust networking domain, autonomic nodes directly communicate with each other. Autonomic nodes can discover other nodes at the same trust networking domain. It requires control or management information between autonomic nodes and control/management plane. It can be pre-configured during bootstrapping. The control information between autonomic nodes can be used to identify the trust networking domain. The autonomic nodes can easily communicate with each other at the same trust networking domain by enabling self-managing capability of autonomic networking. The autonomic service agents can be implemented for trusted communication.

5.4. Communication between trusted autonomic nodes and external nodes

Autonomic nodes must communicate with autonomic nodes of the different trust networking domain. They also communicate with the non-autonomic nodes.

Trust gateway can help that an autonomic node communicate with the autonomic nodes with different trust networking domain or the non-autonomic nodes. Some autonomic service agents (ASA) may include the trust gateway functions for communicating autonomic nodes with different trust networking domain, which is in the reference model for Autonomic Networking [I-D.ietf-anima-reference-model].

6. Trust Networking in the Autonomic Networking Infrastructure

This section describes trust networking of autonomic network. Within a trust networking domain, an autonomic node is credited by their trust level from management plane.

The trust management plane maintains the trust information tables up to date. The trust management plane is tracking of trust status of each autonomic node as an application of autonomic networking. The trust information table contains the trust information of autonomic nodes based on the trust networking domain. All the interactions between autonomic nodes should be verified according to trust evaluation procedures of management plane.

The autonomic nodes within the same trust networking domain create and maintain network connectivity without additional complexity. Trust provisioning among autonomic nodes is to exempt any additional processing (like identification, addressing, routing, forwarding, and security, etc.) to maintain autonomic networking within the same trust networking domain.

The interactions between autonomic nodes are based on the trust evaluation of the trust networking domain. The trust information is used to leverage the direct interactions between autonomic nodes. Trust gateway can help to the interaction of autonomic nodes with different trust networking domains or with non-autonomic nodes.

The trust management plane is used to handle the trust level of each autonomic node with proper trust evaluation procedure.

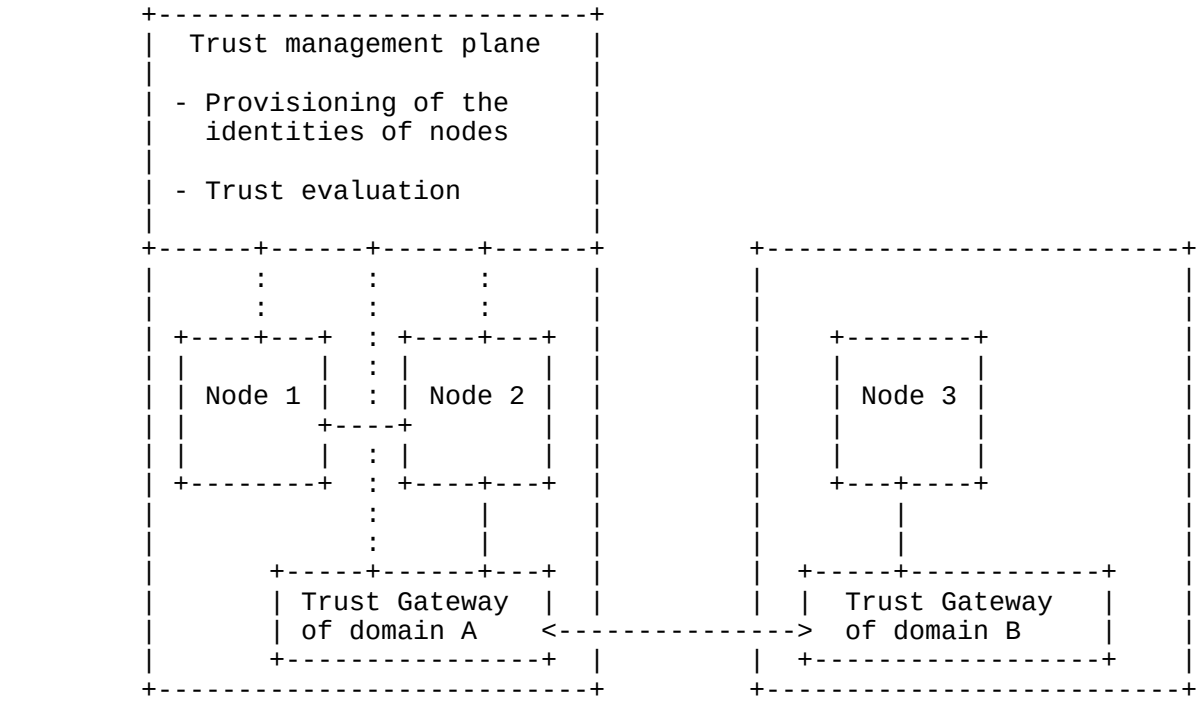


Figure 6. Trust provisioning at the Autonomic Networking

6.1. Identification of Trust networking domain and Trusted Autonomic Node

This section describes trust level. An autonomic node can initiate to create their own trust networking domain. The management plane provides that an autonomic node can build the relevant trust networking domain by identifying the corresponding autonomic nodes. Specific policies can be applied to build trust networking domain.

In a trust networking domain, each autonomic node should be identified by the relevant naming and addressing schemes, which are also compliant with the Reference Model for Autonomic Networking [I-D.ietf-anima-reference-model]. Before data exchange, the autonomic nodes obtains the identities (e.g., IP address and port number,

etc.) of destination nodes and the corresponding trust networking domain. In a case, the MAC address can be also used for identification.

The trust management information database is used for the discovery of autonomic nodes at the same trust networking domain. The autonomic nodes with the same trust networking domain may use the relevant identification schemes. In the trust management information database, a list of autonomic nodes are classified into the relevant identification code which indicates the same trust networking domain. The identification code for a trust networking domain may contain name/nickname and number as well as IP address and port number, etc.

6.2. Discovery of Trust networking domain

The trust management information database is used for the discovery of autonomic nodes at the same trust networking domain. Before data exchange, an autonomic node looks up the trust management information database to find the destination autonomic nodes. If the destination node belongs to the same trust networking domain with original autonomic node, it is possible to initiate data exchange.

6.3. Signaling Between Trusted Autonomic Nodes

At the same trust networking domain, an autonomic nodes communicate with each other. For data exchange, the autonomic node should discover each other by accessing the trust management information database of management plane.

After discovery of destination autonomic node, the signaling protocol like "A Generic Autonomic Signaling Protocol (GRASP)" [I-D.ietf-anima-grasp] are needed to initiate data exchange. Within the same trust networking domain, an autonomic node directly communicates with each other after completing signaling procedure, in which the connectivity among autonomic nodes are securely and automatically maintained. The pre-configuration between autonomic nodes can be done during bootstrapping. The autonomic control plane at the Reference Model for Autonomic Networking [I-D.ietf-anima-reference-model] can be either implemented to carry signaling protocol.

For data exchange with different trust networking domains or non-autonomic nodes, the trust gateway provides proper interworking

functions for data exchange and signaling since there is no direct communication paths between them. The trust gateway provides the relevant control and management information to extend data exchange with different trust networking domains or non-autonomic nodes. The authentication and certificate procedures equivalent with the trust networking domain can be applicable to provide external connectivity.

6.4. Trust Evaluation

Trust evaluation of network is the way of calculating trust for networking services. It requires data collection from various sources. Physical data sources are collected from the capability of data processing, storage, and communication through network. In cyber world, logical data sources are software that work on computing algorithm, storage, and networking. In the social world, human produces various data through user interfaces.

In the physical network, trust can be measured by counting on their trustworthiness of network elements. In the cyber world, software can be accidentally or maliciously altered or destroyed during control, computing, and communicating instances. The unexpected behaviors of software is detected or monitored to evaluate and update their trust level. In the social world, human behaviors can be measured by considering its trustworthiness in terms of ability, honesty and benevolence. Social trust reflects individual human activity. Human interacts with others honestly and kindly so that their trust level is affected by some risks.
For trust evaluation, the collected data are categorized into two types of attributes and indicators namely, qualitative and quantitative. Trust index is used to calculate the certain trust level of each network entity. As the results of trust evaluation, trustor finally make a decision. The network management plane provides to calculate the trust level of the network elements from various data sources and store their values to trust management information database.

The trust management information contains the trust level of autonomic nodes. The interactions inside a trust networking domain are analyzed and accumulated to evaluate the trust level of each node. The trust level of autonomic node is contained at the trust

management information database. All the interactions between autonomic nodes in a same trust networking domain is validated by the trust evaluation procedure.

The trust evaluation procedure is fed by the following inputs.

- o Pre-provisioned or manually configured by policy or management information
- o Analysis from interactions between autonomic nodes
- o The accumulated history information of trust verifications such as authentication of non-autonomic nodes and validity of application specific transactions.
- o other unaccepted or unexpected behaviors

While autonomic nodes communicate with each other, they choose the relevant trust management protocol whether they meet trust requirements in the same trust networking domain or not. Trust management protocol between autonomic nodes and trust management database is needed to check trust evaluation. Trust evaluation procedure between autonomic nodes at same trust networking domain are taken for trust identification.
If the prerequisite and pre-configuration procedures are already taken for trust management, simple and light-weight solution can be applicable for communication between autonomic nodes.

7. Procedures for trust networking

7.1. Building a trust networking domain

7.1.1. Domain initialization

To build a new trust networking domain, the domain administrator needs to initiate the functionalities of trust networking domain as follows:

- Domain administration
To initialize a domain with respect to the trust, the domain administrator needs to configure policies of trust and membership. To manage the trust level, the domain administrator sets the

required trust level of membership with domain policy management (DPM) ASA. The domain administrator can explicitly dedicate a node for trust management functions and trust provisioning.

- Access & delivery control
  The nodes that connected outside of the domain should equip trust gateway functions. For IP network case, every node of the domain should assign their gateway to the nodes with trust gateway ASA.

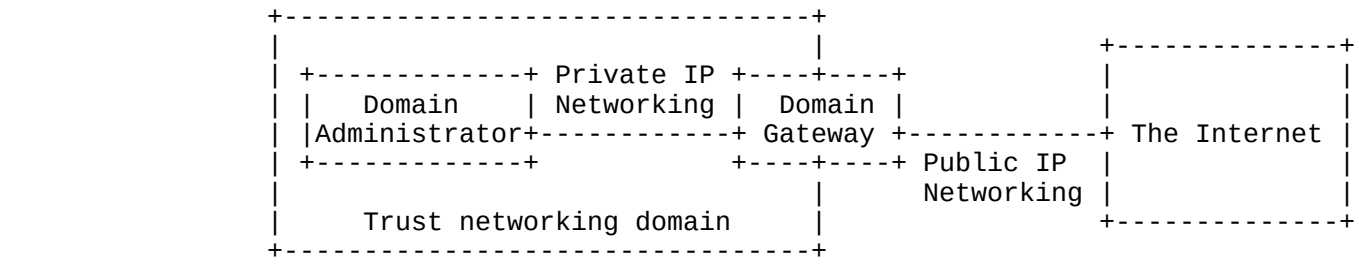


Figure 7. Initialization of a new trust networking domain

7.1.2. Node registration

After the trust networking domain has been initialized, domain can adopt network nodes.

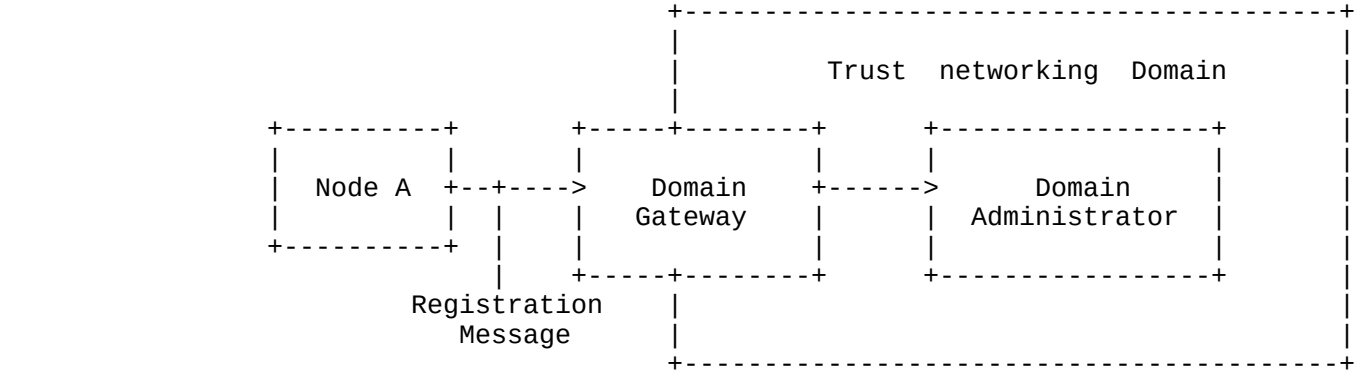


Figure 8. Registration of a new node

The procedures of node registration are as follows:

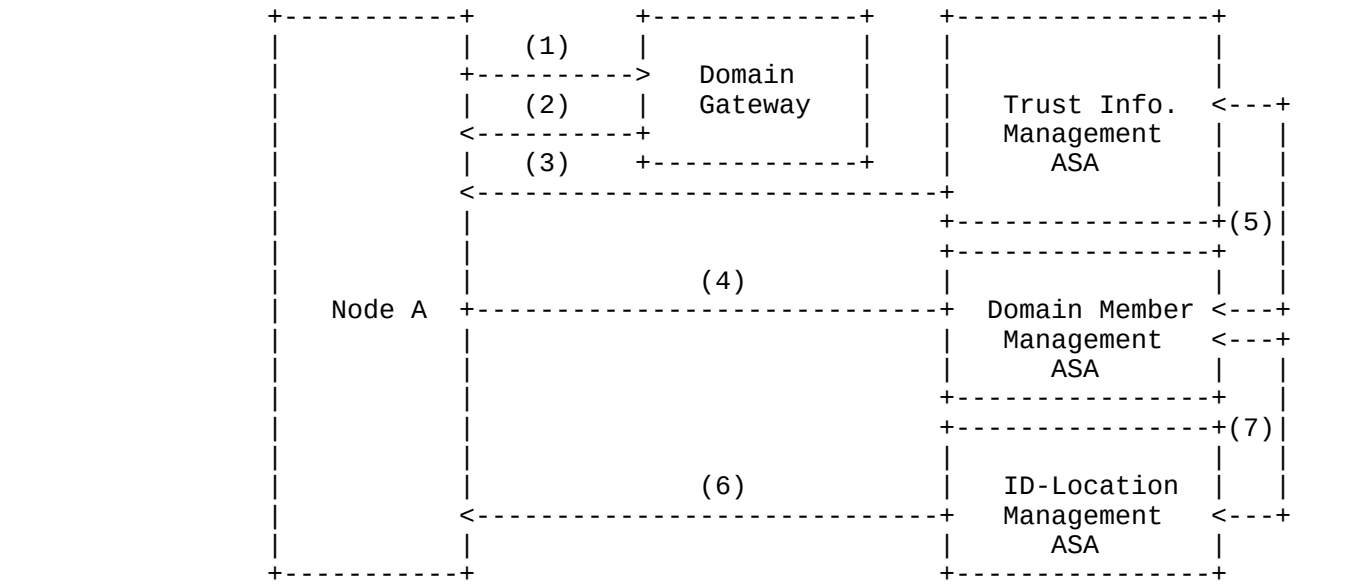


Figure 9. Procedures of node registration

(1) Node A connects to the network of trust networking domain;
(2) The domain assigns a private IP address to Node A. The domain gateway is assigned as the default gateway for IP network;
(3) Trust information management ASA analyses the trust information of node A;
(4) Node A request to join the domain;
(5) Domain membership management ASA of the domain administrator receives the requests and decides to approve Node A, based on the domain policy and trust level of Node A;
(6) ID-Location management ASA of the domain administrator issues a new identifier of Node A;
(7) ID-Location management ASA archives Node A’s identifier and private IP address.

7.2. Evicting existing node from trust networking domain

(Editors' note) This section describes how to evict existing node in trust networking domain including trust management procedures. Further details are for further study.

7.3. Terminating trust networking domain

(Editors' note) This section describes how to terminate trust networking domain including signalling procedures with child nodes (or domains) and parent domains. Further details are for further study.

7.4. Communication among trust networking domains

This section describes trustworthy communication between nodes within a single trust networking domain and between nodes separated into multiple trust networking domains.

7.4.1. Trustworthy networking within a single trust networking domain

In order for the two hosts to send and receive messages to each other, a networking path must first be established. If two hosts are located in the same domain, they already have trust relationship with each other which means no additional security procedures are needed.

7.4.2. Trustworthy networking between trust networking domains

Two hosts are in different domains. It means that they do not know each other's IP address directly. The domain administrator provides IP address of each hosts for trustworthy networking between two hosts in different domains. If a Host 2 wants to perform trustworthy networking with a Host 1 in other domain, it is possible to establish a networking path between two nodes through interactions between domain administration functions and access and delivery control functions. Figure 10 shows an overview of trustworthy networking between trust networking domains.

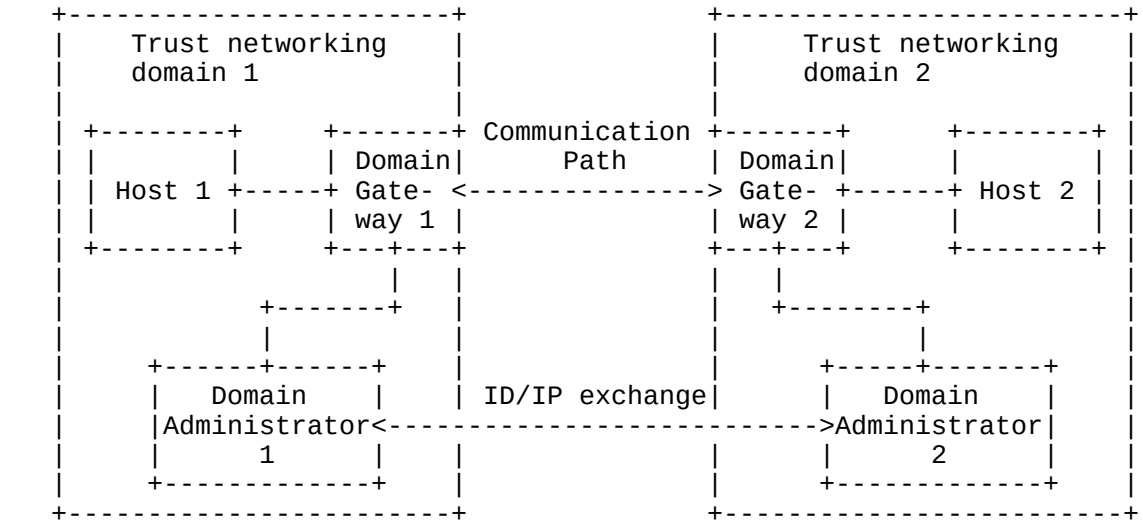


Figure 10. Trustworthy networking between trust networking domains

Figure 11 shows detailed procedures for trustworthy networking between trust networking domains are follows:

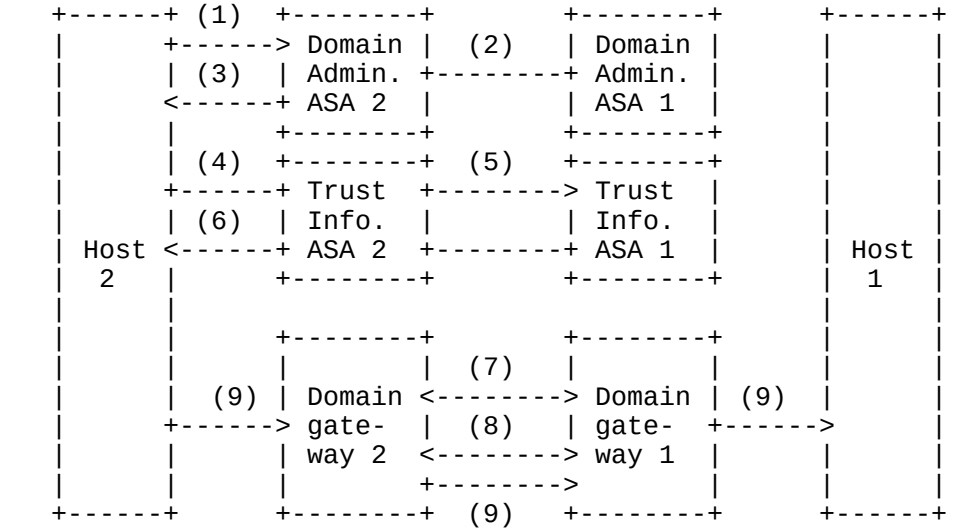


Figure 11. Procedures of trustworthy networking between trust networking domains

(1) Host 2 requests IP address of Host 1 to the domain administration ASA 2 through the ID of the host 1;
(2) The domain administration ASA 2 requests IP address of the Host 1 to the domain administration ASA 1;
(3) The domain administration ASA 1 obtains IP address of the Host 1 and reply ID and IP address of the Host 1 to domain administration ASA 2, and it replies to Host 2;
(4) Host 2 requests a trust level of Host 1 through the domain administration ASA 2;
(5) The domain administration ASA 2 checks a trust level of Host 2 through the trust information management ASA and requests a trust level of Host 1 to domain administration ASA 1;
(6) The domain administration function 1 obtains the trust level of Host 1 through the trust information management ASA and replies it to the domain administration ASA 2, and the result replies to Host 2;
(7) The access and delivery control ASA 2 forms a routing path with the access and delivery control function 1 through the ID-based routing ASA;
(8) The Host 2 and the Host 1 establish a reliable link through the domain gateway ASA of each trust networking domain;
(9) Networking path established between Host 1 and Host 2.

8. Security Considerations

Data exchange between autonomic nodes at the trust networking domain must be secured. The signaling or management protocols for trust identification and discovery of trust networking domain are secure. The control/management plane for trust management is self-protecting. The autonomic node in a trust networking domain should be certified by its identity. The pre-configuration information of autonomic nodes from trust management information database should be certified during bootstrapping time.
For data exchange with different trust networking domain or non-autonomic network, the trust gateway should be securely implemented. Trust gateway maintains the same trust level for cross-domain applications or interaction with non-autonomic network.

9. IANA Considerations

This document requests no action by IANA.

10. Acknowledgements

11. Contributors

12. References

12.1. Normative References

[I-D.ietf-anima-autonomic-control-plane]

Eckert,T., Behringer, M., and S. Bjarnason, "An Autonomic Control Plane (ACP)", draft-ietf-anima-autonomic-control-plane-13 (work in prgress), December 2017.

[I-D.ietf-anima-grasp]

Bormann, C., Carpenter, B., and B. Liu, "A Generic Autonomic Signaling Protocol (GRASP)", draft-ietf-anima-grasp-15 (work in progress), April 2018.

[ITU-T Y.3052] Overview of trust provisioning in information and communication technology infrastructures and service, March 2017

[ITU-T Y.3053] Framework of trustworthy networking with trust-centric network domains, January 2018

12.2. Informative References

[I-D.ietf-anima-reference-model]

Behringer, M., Carpenter, B., Eckert, T., Ciavaglia, L., Pierre, P., Liu, B., Nobre, J., and J. Strassner, "A Reference Model for Autonomic Networking", draft-ietf-anima-reference-model-08 (work in progress), February 2018.

Authors' Addresses

Tae Sang Choi
Electronics and Telecommunication Research Institute (ETRI)
218 Gajeong-ro, Gajeong-dong, Yuseong-gu, Daejeon
Korea

Email: choits@etri.re.kr

Jun Kyun Choi (editor)
Korea Advanced Institute of Science and Technology (KAIST)
193 Munji Ro, Yuseong-gu, Daejeon
Korea

Email: jkchoi59@kaist.ac.kr

Tae Su Jeong
Electronics and Telecommunication Research Institute (ETRI)
218 Gajeong-ro, Gajeong-dong, Yuseong-gu, Daejeon
Korea

Email: tsjeong@etri.re.kr

Nam Seok Ko
Electronics and Telecommunication Research Institute (ETRI)
218 Gajeong-ro, Gajeong-dong, Yuseong-gu, Daejeon
Korea

Email: nsko@etri.re.kr

Jae Seob Han
Korea Advanced Institute of Science and Technology (KAIST)
193 Munji Ro, Yuseong-gu, Daejeon
Korea

Email: j89449@kaist.ac.kr