WP4: Supporting Communities in Programmable Grid Networks: gTBN

The generalised Token Based Networking (gTBN) architecture enables dynamic binding of communities and their applications to specialised network services. gTBN uses protocol independent tokens to provide decoupling of authorisation from time of usage as well as identification of network traffic. The tokenised traffic allows specialised software components uploaded into network elements to execute services specific to communities.

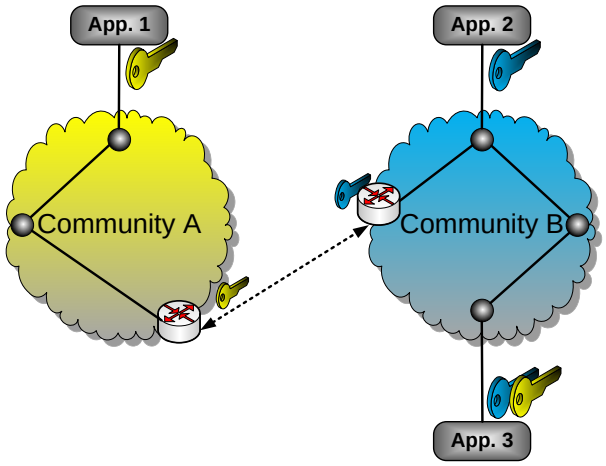

Figure 1. The gTBN architecture.

Figure 1 shows an example application of gTBN. Two communities with its member applications are located on different network domains. For example, Application 2 and 3 belong to community B, and Application 1 belongs to community A. The two communities are each associated with a token, yellow and blue, respectively. Let us assume that the policy of a network domain is that only members of the communities are allowed to be routed through the network. Application 2 and Application 3 are both members of community B and therefore, they can communicate. Correctly tokenised traffic will be routed using default IP mechanisms. However, to communicate with Application 1, Application 3 also needs credentials to access the resources of community A. gTBN supports binding of multiple domain-specific services into a single token. This allows a member of both communities A and B to access each other's network domains.

Use Case: multiple applications share common network resources

The Token Based Network (TBN) testbed uses Token Based Switch over IP (TBS-IP) as a low-level system for traffic switching at high speeds (multi gigabits/sec) based on packet authentication. TBS-IP helps high-performance computing and grid applications that require high bandwidth links between grid nodes to use priority links for authorised packets with policy constraints. TBS-IP is fast and safe and uses the latest network processor generation (Intel IXP2850). Figure 2 shows an overview of how the TBN tesbed is plugged into the Phosphorus GMPLS testbed. The TBN testbed works as a separate network domain, located at University of Amsterdam (UvA-TBN), which interconnects an entire UvA IP campus network into the GMPLS testbed. In other words, applications running on various hosts connected within UvA IP campus network may request, and authorise to use GMPLS lightpaths towards other end-points into the European Phosphorus testbed, such as I2CAT (Barcelona), or VIOLA (Bonn).

Note that in this testbed, TBS-IP works as a gateway router between IP networks and GMPLS circuits, and therefore, the mapping of IP over GMPLS uses specific AAA authorisation sequences implemented by a high-level authority, Harmony, at service plane. An example of authorization sequence is described below.

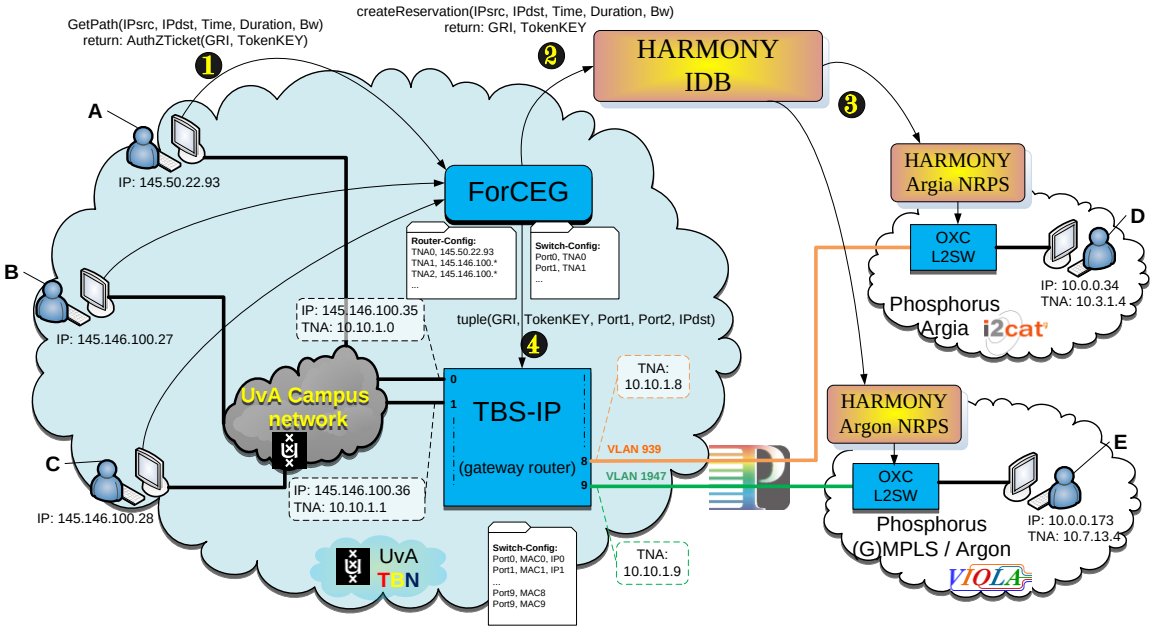

Figure 2. TBN-UvA demo within Phosphorus testbed

Specific user applications (e.g., VLC server) from IP campus network may want to connect to VLC-clients located in other network domains interconnected over GMPLS as in Figure 2. The work-flow of authorisation of the user-applications to use network services uses the following steps:

1. User application requests to the UvA-TBN gateway router (ForCEG service in Figure2) a path between the IP addresses (IPsrc, IPdst, startTime, duration, bandwidth), where IPsrc must be within its IP campus network, and IPdst should be available within the GMPLS networks.
2. The ForCEG service will authenticate the user application and request a path to the GMPLS authority (IDB in Figure2) on behalf of its user applications. As a result, IDB will generate and return the credentials of using authorised paths in format of a Global Reservation Identifier (GRI) and a TokenKey used of in-band encryption.
3. IDB will prepare all intermediate domains involved in the path provisioning with the requested credentials (GRI, TokenKey, etc).
4. Once the start-time of the requested path arrives, the received credentials from IDB are enforced into the TBS-IP gateway router at the lowest level (IP packets and circuits).
5. When a user application (e.g., vlc) is authorised to connect to a IPdst over GMPLS network, the magic-carpet environment inserts encrypted tokens within the outgoing packets (media streams) and redirect them towards TBS-IP.
6. TBS-IP authenticates every received packet identified by the plain-text GRI as a lookup computation (finds GRI-entry into the local AuthZ-table), then it does:
    a. If the Packet comes from IPcampus network (PKT.IPdst==GRI-entry.Port1.IPaddr), then it will re-write its IPdst to the correct endpoint (PKT.IPdst=GRI-entry.IPdst) and will push the packet into the proper GMPLS path, as indicated by GRI-entry.Port2;
    b. If the Packet comes from GMPLS network (PKT.IPdst!=GRI-entry.Port2.IPaddr), then it will push the packet into the proper outgoing port into IPcampus as indicated by GRI-entry.Port1;

Contact: : Mihai Lucian Cristea, m.l.cristea@uva.nl, www.cristomatics.eu