5. Integration of legacy access networks into the 5G Core network

This section describes a solution to be developed in the scope of NEXUS WP6 for the integration of non-5G capable devices into a 5G network.

5.1. Context

Wireline-Wireless Convergence (WWC) or *Fixed and Mobile Convergence* (FMC), has long been addressed by 3GPP [61] and other organizations like the Broadband Forum (BBF) [62], defining solutions for a shared mobile core, serving wired and wireless access technologies. Already addressed in 4G/LTE scope, this gained higher relevance with 5G, due to its intended broader scope.

With 5G, convergence is achieved at the core, devised as being access agnostic, meaning that its core elements are able to integrate access technologies other than 5G-NR, via gNB Access Nodes (AN), and LTE, via ng-eNB. This is achieved by the complementary help of additional functional entities placed at the 5G domain entrance, which adapt access specific protocols to standard N2 (control plane) and N3 (data plane) interfaces. In these scenarios, mobile terminal equipment has 5G credentials and support the N1 interface.

The N1 interface (used to convey non-radio signalling between the mobile terminal equipment and the 5GC) may not be supported by the end systems, as is the of non 5G capable devices, forcing the adaptation entities to handle it on behalf of the terminal; that is the case for most of the fixed network residential gateways (FN-RGs), as defined by BBF.

5.2. Advantages

Convergence enables multi-technology endpoints to choose the access technology to use at each time (traffic steering and switching) and even to connect simultaneously via different access technologies (traffic splitting). Started with Multi-Radio Dual Connectivity (MR-DC) in Release 15, this is now specified as AT-SSS (or AT-3S, for *Access Traffic Steering, Switching and Splitting*), currently part of 5G standards (see the specific section below on this topic).

Besides that, WWC brings other potential advantages:

1. Common and consistent authentication/registration and global assignment of security policies, even if indirectly.

2. Consistent traffic management (e.g. routing, forwarding, inspection, policy enforcement, QoS handling and reporting) across all access types, via UPF functions.
3. Common IP address management policies, managed between the 5GCore (SMF), Interworking Function (IWF) and GTW.
4. Multi-access technology Slicing/Virtual networking management, with IoT devices being grouped and be part of extended virtual networks or *hyperslices*, made of 5G slices, Ethernet VLAN, and WLAN Service Set Identifier (SSID).
5. Common interface for OAM operations.
6. Exposure to external entities as a single network.

5.3. 5G access nodes

3GPP defines two native 5G access nodes (see Figure 2):

1. **gNB**, for pure 5G-NR accesses
2. **ng-eNB**, for LTE accesses

With these, 5G and 4G terminals respectively, are able to access services with the support of a 5G Core, without the need for additional functional entities. However, other access node types have been defined to integrate other type of accesses in 5G Cores:

1. **N3IWF (*Non-3GPP Interworking Function*)**

   Allows 5G capable terminals (supporting NAS) to connect from untrusted WLANs or other accesses deployed by third-party entities, out of the scope of 5G network owner control.

   Establishes IP Sec sessions for the control and user planes, with devices to be connected, that way allowing NAS (N1) signalling to be directly exchanged with the 5G Core (AMF).

   Thus, the usage of N3IWF requires devices to have 5G credentials and be able to establish IPSec tunnels with the interworking function.

2. **TNGF (*Trusted Non-3GPP Gateway Function*) and TWIF (*Trusted WLAN Interworking Function*)**

   For trusted non-3GPP and WLAN accesses, but requiring the UE to have 3GPP credentials and, for the first case, to support NAS (N1).

   Based on the tight coupling between a trusted Access-Point and a gateway or interworking function; IPSec is also used here.

3. W-AGF (Wireline Access Gateway Function)

   Connects a Wireline 5G Access Network (W-5GAN) to the 5G Core Network.

   Like the TNGF for 5G Residential Gateways (5G-RGs) and to the TWIF for Fixed-Network Residential Gateways (FN-RGs) but considering the specific characteristics of fixed access networks.

   5G-RG units support NAS signalling and authenticate themselves, while FN-RG do not support 5G capabilities and do not have 3GPP credentials, in this specific context. The W-AGF derives identifiers from the used access characteristics.

When started, Access Nodes need to establish connectivity with the 5G Core (AMF) and with other surrounding gNBs (if the network supports handovers via Xn interface). In the process, they shared several parameters, one being its Access None type. The core will then interact with that element according to its type. For the moment, 5G Cores in general only support gNB Access Nodes.

Complementary, is the same area of authentication and authorization, 3GPP defined the NSSAAF (*Network Slice Specific Authentication and Authorization Function*), which manages whenever required specific secondary, external per slice authentication and authorization, as the name implies. In such cases, AMF acts as a proxy for EAP between the terminal (UE) and the NSSAAF, and from the latter to an external AAA.

5G also introduced AKMA (*Authentication and Key Management for Application*) for securing the communication between UEs and AFs (*Application Functions*), based on the same primary 5G authentication, eliminating the need for a second authentication in front service platforms.

5.4. Existing prototype

The work to be conducted shall improve and extend an existing prototype of the target Interworking Function (IWF). The IWF corresponds to a BBF AGF for FN-RG but presenting itself to the 5G Core as a gNB, thus eliminating the need for the 5G Cores to recognize other Access Node types. It promotes, in a simplified and universal way, convergence between 5G and Ethernet based accesses, e.g. WLAN.

The existing IWF does not required devices to establish IPSec tunnels and mobile terminals to have 5G credentials. For that purpose, the IWF is provisioned with a set of 5G credentials, also provisioned at the 5G core, which are used whenever a non 5G capable terminal requires data access. That process is triggered by Dynamic Host Configuration Protocol (DHCP), requiring the IWF to be the DHCP server of the IP segment the device is connected to, being the presented MAC

address used as the ID of the device and mapped to an available 5G identifier. This mapping can be made static. Currently, only connection to a single slide is considered.

It follows *Software Defined Networking* (SDN) principles and mechanisms to map WLAN connections to 5G sessions, under the common control of a single instance of 5G Core composed of three main blocks, which are depicted in Figure 33:

1. SDN controller and interworking function emulation
   - Responsible for intercepting protocol packets on the LAN (e.g. DHCP), mapping clients (MAC addresses) into particular SUPIs and trigger the allocation of UEs on the 5G network.
   - Controls the data plane for bridging traffic into the UPF.
   - It is externally controlled via REST, emulates a router/ Broadband Network Gateway (BNG) on the Fixed Network side.

2. gRPC
   - Responsible for receiving the allocations and deallocations on the 5G network. Interacts with the RAN, emulating the Next Generation Application Protocol (NGAP) protocol.
3. Data plane
   - Bridges traffic from the LAN to the UPF (layer 3), via standard N3 interface, which requires General Packet Radio Service Tunnelling Protocol (GTP) encapsulation.

From above, there is no security mechanisms to properly authenticate and authorize non 5G devices. Only the observed MAC address, which can be forged, is used to identify the device and assign to it a 5G identity.

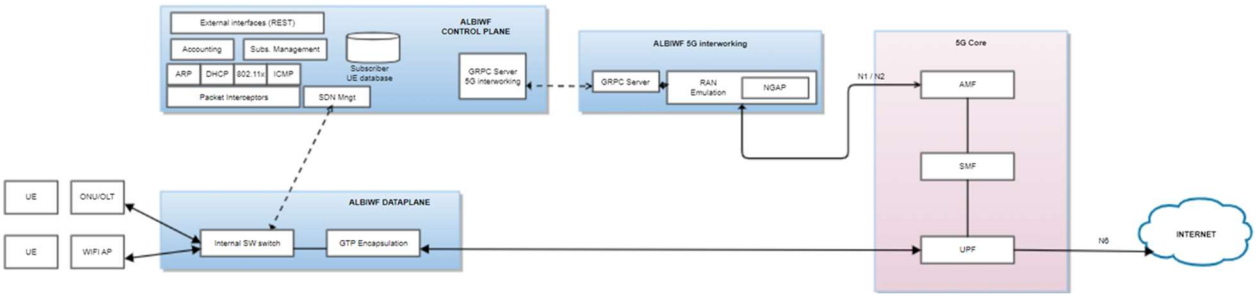

Figure 33 - IWF main blocks (developed by the authors).

5.5. Functional expansion

The existing prototype will be functionally extended to improve security and extend 5G slicing concept with WLAN SSIDs or Ethernet VLAN as described in the following.

5.5.1. Improve non-5G devices authentication and authorization (AA) mechanisms

Integration of other wired and wireless access authentication and authorization protocols with 5G ones. 5G uses 5G-AKA and EAP-AKA' for primary authentication, both of which can be executed over 3GPP access and non-3GPP access when end devices support them.

N3IWF, TNGF and TWIF require devices to have 5G credentials in order to have a single point of provisioning. With the existing prototype, the IWF needs also be provisioned what is not considered a limitation since this can be easily implemented by supporting information systems via an appropriate API.

The foreseen solution to improve the authentication and authorization process, keeping it generic, is based on the interception of the RADIUS traffic between the authenticating entity (e.g. the Authenticator in 802.1x) and the respective RADIUS server. This allows the extraction of the device identity and obtain the result of the process. Changes in the current device identity definition are required since the DHCP process may no longer be controlled by the IWF.

5.5.2. Integrate Zero Trust principles

The objective is to grant access to the remote resources following Zero Trust principles. 5G provides QoS control via PCF and access to slices via NSSF, based on UE provisioned profile. Apart from that, 5G provides transparent, universal connectivity to all IP destination reachable by the DNN provided connectivity to. It does not provide a more granular, per flow (IP address origin/destination, transport protocol and TCP/UDP origin/destination ports) access control.

With this functional improvement, after the device gets authenticated, authorization to access remote resources need to be granted in a need to access principle. The IWF needs to intercept the device traffic and check its origin and destination against defined rules.

5.5.3. Implement ‘extended slices’

The objective is to create ‘extended slices’ by joining 5G Slices, identified by SSD/SD, WLAN ESS, identified by SSID, and Ethernet VLAN, identified by VLANID. Connectivity between devices is controlled in a per ‘extended slice’ basis, as if they were all in the same Slice, ESS or VLAN, from their point of view.

For this to happen, first, a static mapping between devices IDs and 5G IDs must be supported and provisioned in the IWF. Then the IWF must be enriched with information defining how connectivity is granted to the device from the WLAN SSID or Ethernet VLAN to existing 5G Slices, as presented in Figure 34.

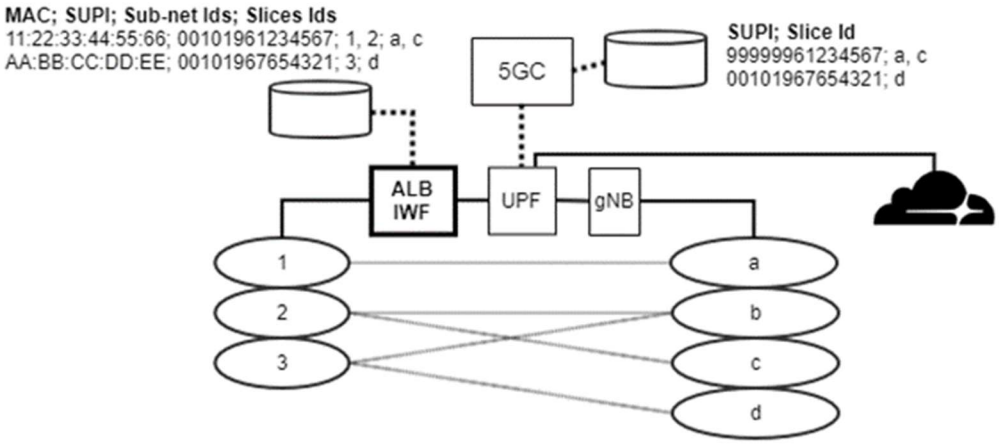

Figure 34 - IWF extended slices management (developed by the authors).