Discussions & Clarifications

Topics

- **6.1 Whether it will bring privacy issue? If yes, how to overcome?**
- **6.2 Whether it will bring security issue? If yes, how to overcome?**

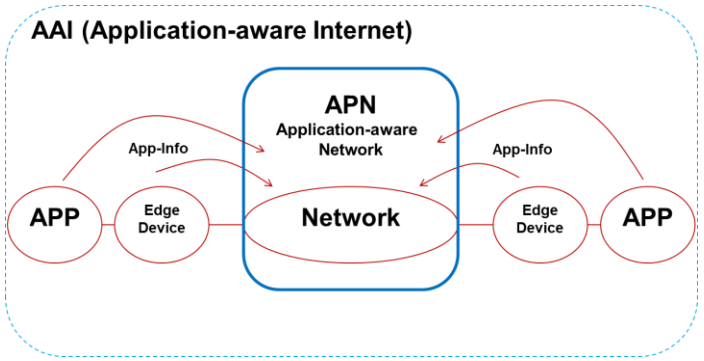
Privacy Issues

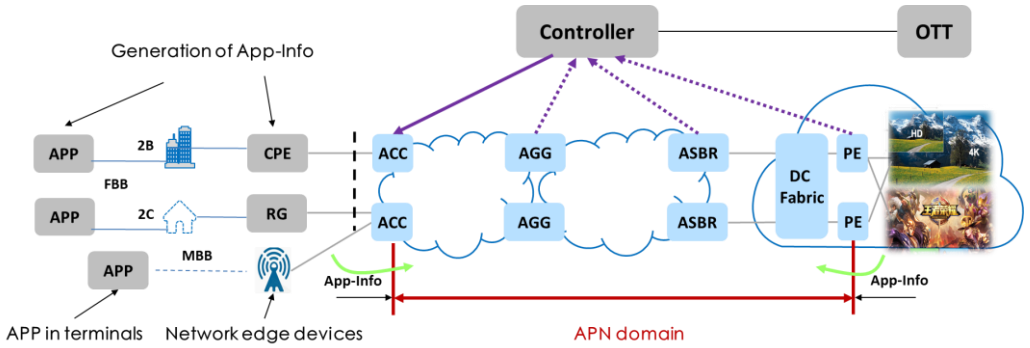
- Scenarios

1. **No privacy issue**: Operators run their own applications – e.g. CMCC MIGU Music
2. **No privacy issue**: App providers build and run their own networks – e.g. Google B4
3. **No privacy issue**: APN works only within an operator’ s controlled limited domain no matter where the App-info is added and encapsulated.
4. **No privacy issue**: If added at the edge device (i.e. an network operator-controlled device), e.g. Enterprise CPE or Home broadband RG or BNG or WiFi AP or 5GC UPF.
5. **No privacy issue**: If added at the APP, the App-info is encrypted.
6. **May have privacy issue**: If added at the APP, the explicit App-info is not encrypted.

Google’s Data Center WAN (B4 Network)

1. Google controls
   - applications,
   - Servers,
   - LANs, all the way to the edge of network
2. bandwidth-intensive apps
   - Perform large-scale data copies from one site to another;
   - Adapt transmission rate
   - Defer to higher priority interactive apps during failure periods or resource constraints
3. No more than few dozen data center deployments, hence making central control of bandwidth possible



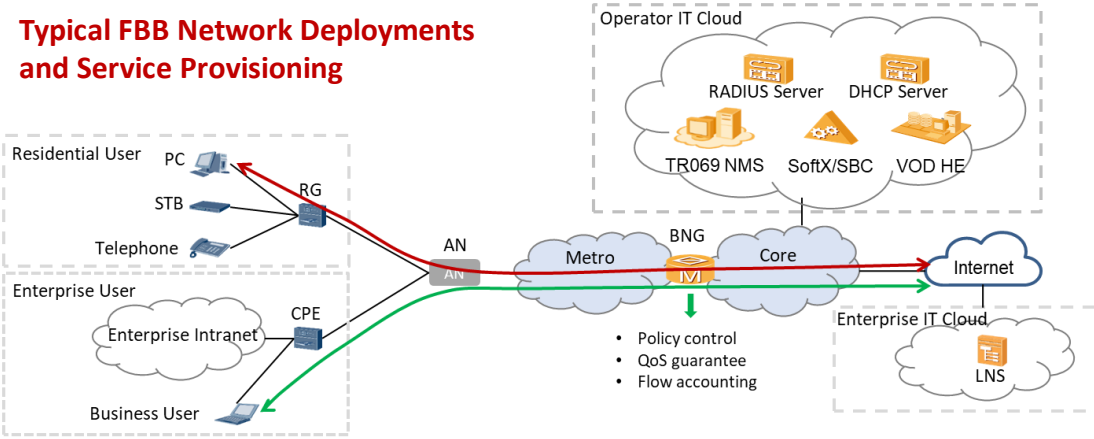


Security Issues

- No Security Issue: Inter-DC scenario
- No Security Issue: Enterprise scenario, access through a controlled BNG interface
- APN only imposes security issues when users access from an untrusted domain, but
  - **Home broadband scenario** can be validated via BNG
  - **Mobile broadband scenario** can be validated via 5GC
- APN potentially imposes four types of security issues

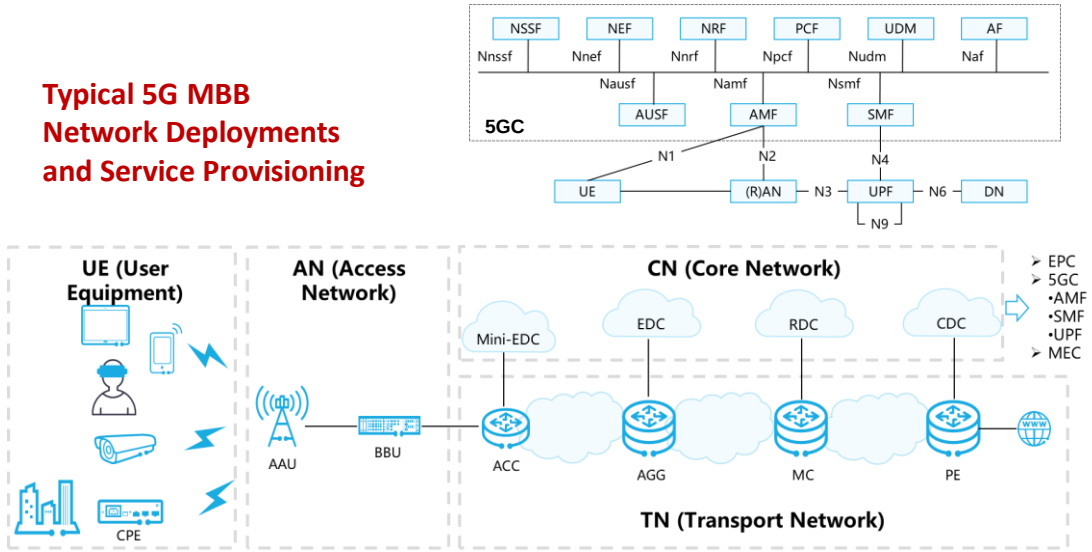
1. Within one terminal – can be tackled via OS; blocked via BNG or 5GC
   a) An application in one terminal (UE) adds arbitrary App-Info (incl. Request)
   b) An application in one terminal adds the App-Info of the other App in the same terminal
2. Once sent out it will be validated via Network-side security solutions
   a) An application in one terminal forges the App-Info of the same App in another terminal
   b) App-Info is tampered along the way between the App-Info creator and the Network Boundary

Typical FBB Network Deployments and Service Provisioning

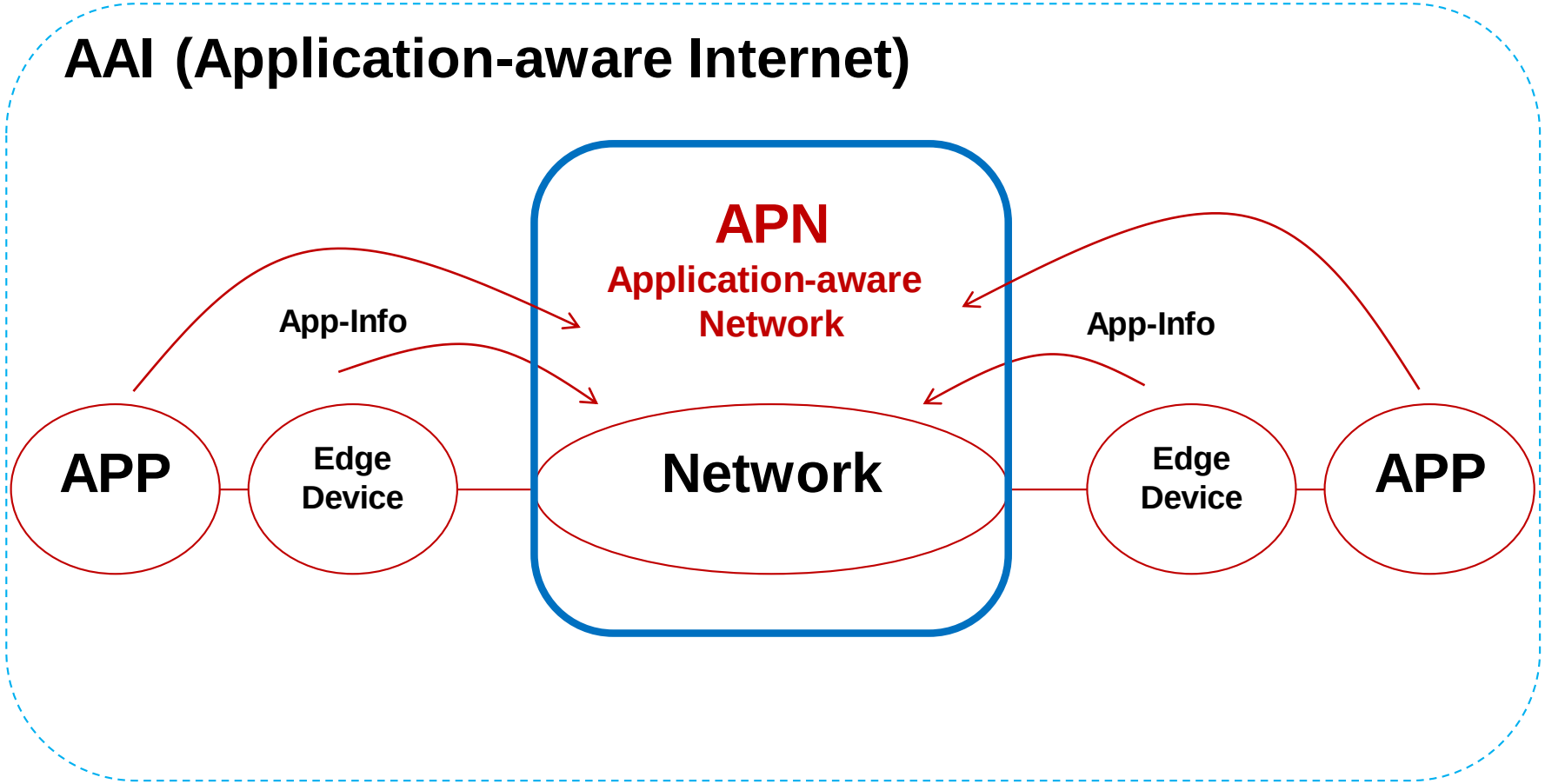


BNG as a gateway to provide user access, AAA, and value-added services.

Typical 5G MBB Network Deployments and Service Provisioning

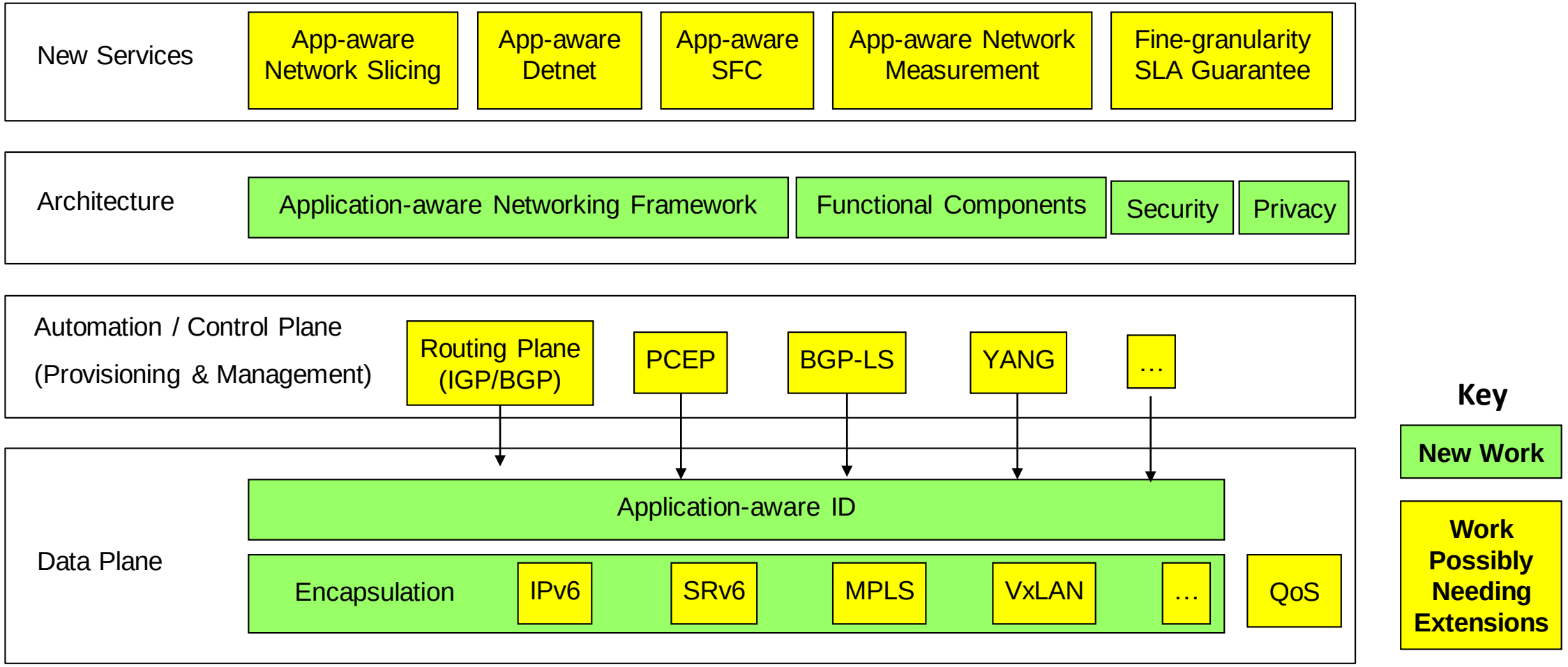


APN Scope



The focus of APN is going to be within the Application-aware Network Domain in the scenarios with no privacy and security issues.

Work Items in APN



Shaping the APN Discussion

- Are the right use cases identified?
- What techniques are available to achieve the goals of the use cases?
- Can we ensure the scope of work to focus on a limited number of domains, and the network layer?
- How can we address security and privacy issues?
- If there is interest in continuing the work? If so, where would we do this work, RTG Area, or?
  - Encapsulation of application related information in MPLS, IPv6, SRv6, VXLAN, etc.
  - Distribute application related information through IGP/BGP/PCEP extensions.