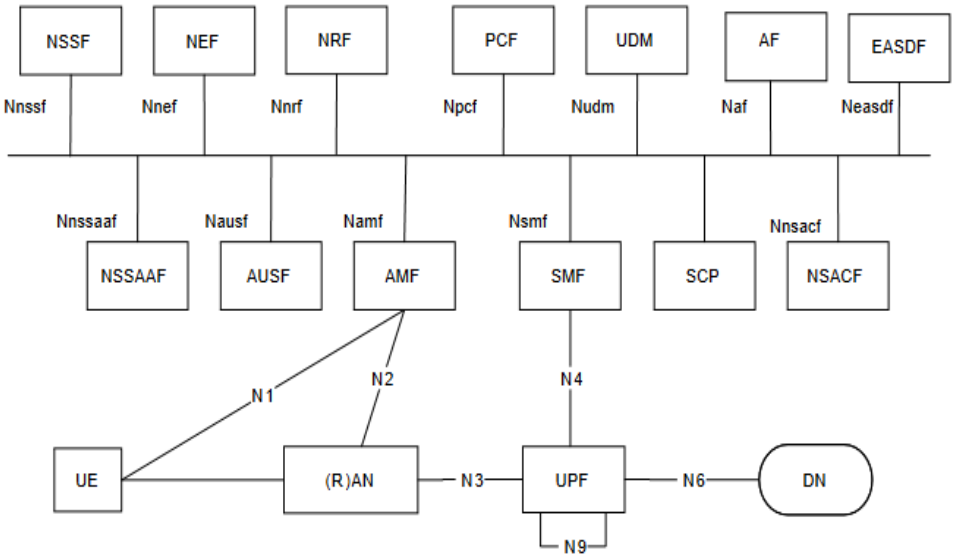
4.2.3 Non-roaming reference architecture

Figure 4.2.3-1 depicts the non-roaming reference architecture. Service-based interfaces are used within the Control Plane.



Network Function functional description-->

1. AMF->

It is stands for access and mobility Management Function.

a. Access Management->

AMF handles the initial access of user to the 5G network. It manages procedures such as authentication, authorization, and security setup when a device connects to the network.

b. Mobility Management->

It refers to the technology and processes that enable your phone or other devices to stay connected and maintain a stable signal as you move around.

When you move from one area (covered by one base station) to another (covered by a different base station), your device needs to switch its connection. Mobility management makes sure this handover happens smoothly, so your call or data session doesn't get interrupted.It also helps optimize your connection by choosing the best base station for your device at any given moment.

functionality-->

Termination of Ran CP Interface
Termination of NAS
Connection Management
Registration Management
Reachability and Mobility Management
Access Authentication and Authorization

2. SMF->

It Stands for Session Management Function.It plays a crucial role in managing data sessions between user equipment (UE), such as smartphones or IoT devices, and the core network.

functionality->

1. Session Management->

SMF is primarily responsible for establishing, modifying, and terminating data sessions for users. It manages the user plane resources during these sessions.
Bearer Management: It handles the establishment, modification, and deletion of bearers (logical channels) that carry user data through the network.

2. Quality of Service (QoS) Management->

SMF ensures that the required QoS levels are maintained throughout the data session according to the service requirements and network capabilities.

3. Policy Enforcement->

It enforces policies related to data traffic management, ensuring compliance with operator-defined rules for traffic steering, prioritization, and optimization.

4. User Plane Function (UPF) Interaction->

SMF interacts with the User Plane Function (UPF), another crucial component in the 5GC, to route and forward user data packets according to the established session and bearer configurations.

5. Charging Control:->

It collects session-related information for charging purposes, ensuring that data usage is accurately accounted for based on the agreed service plans.

6. SMF works closely with other network functions like the Access and Mobility Management Function (AMF), Authentication Server Function (AUSF), and Network Exposure Function (NEF) to provide end-to-end connectivity and service delivery.SMF is designed to be highly flexible and scalable, capable of handling a large number of data sessions concurrently.

7. It supports network slicing, which allows operators to create multiple virtual networks (slices) within a single physical 5G infrastructure

3. UPF->

Its primary role is to handle and process user data packets as they traverse the network. It is responsible for the actual forwarding and routing of user data packets between the devices (UEs - User

Equipments) and external data networks (such as the internet or enterprise networks).

Functionality->

A. Packet forwarding->

Responsible for routing data packets from the UE to their intended destination.

B. Quality of Service (QoS) enforcement->

Ensures that packets are delivered quickly and reliably, while also prioritizing certain types of traffic.

C. Traffic filtering->

Identifies and blocks certain types of traffic based on predefined policies.

D. Network slicing->

Allows different virtual networks to be created on a single physical network, each with its own set of QoS policies and parameters.

E. Session management->

Sets up and tears down data connections between the UE and the network.

F. Policy enforcement->

Ensures that network policies and rules are followed by all network components.

G. Mobility management->

Determines the best route for data packets to take as the UE moves between different cells or base stations.
Data forwarding: Forwards data packets between the UE and external

network services.

4 PCF->

PCF stands for Policy Control Function. It is a crucial network function within the 5G Core (5GC) architecture responsible for managing and enforcing policy rules related to Quality of Service (QoS), charging, and network resource allocation.

Functionality->

1. Policy Enforcement->

PCF enforces policies that govern how network resources are allocated and managed to meet specific service requirements. This includes defining QoS parameters (e.g., latency, bandwidth) and ensuring that they are maintained during data sessions.

2. Dynamic Policy Control ->

It dynamically adjusts policy rules based on real-time network conditions, user demands, and operator-defined priorities. This allows for adaptive resource allocation and QoS management.

3. Charging and Billing->

PCF interacts with charging systems to gather session-related information for accurate billing and charging purposes. It ensures that users are billed according to their data usage and service agreements.

4. Traffic Steering and Optimization->

PCF supports traffic steering based on policy rules, directing traffic through optimal paths or network segments to enhance performance and efficiency. This includes traffic prioritization and redirection based on application requirements.

5. Integration with Network Slices->

PCF facilitates policy management within network slices,

allowing operators to define and enforce policies tailored to specific service instances or customer segments.

6. Service Awareness->

PCF is service-aware, meaning it can differentiate policies and QoS requirements based on the type of service (e.g., voice, video streaming, IoT applications).

Interaction with Other Functions:
1. SMF (Service Management Function): PCF interacts with SMF to enforce policies related to traffic management, QoS, and session handling.

2. AMF (Access and Mobility Management Function): PCF coordinates with AMF to apply policies based on user context (e.g., location, mobility) and access technology (e.g., 5G NR, Wi-Fi).

3. UPF (User Plane Function): PCF collaborates with UPF to ensure that policy rules are implemented in the user plane for consistent QoS enforcement and traffic management.

4. Support for Network Slicing:PCF supports network slicing by enabling the creation and management of policies specific to each network slice. This allows operators to offer differentiated services with varying QoS levels and resource allocations within a single physical infrastructure

5. NEF->

NEF stands for Network Exposure Function. It is a key component within the 5G Core (5GC) architecture that enables controlled access to network services and capabilities by authorized third-party applications, services, and external networks.
NEF is a network function in the 5G Core Network (5GC) that facilitates

secure and controlled exposure of network capabilities and services to authorized external entities.
It serves as an interface point for external applications and services to interact with the 5G network, enabling them to utilize network resources and provide value-added services.

Functionality->
1 Service Exposure: NEF exposes network services and capabilities (such as QoS policies, subscriber data, session management functions) to authorized third-party applications and service providers through standardized APIs (Application Programming Interfaces).

2 Policy Management: NEF manages and enforces policies related to access control and service usage. It ensures that only authorized entities can access specific network resources and services based on predefined policies and permissions.

3 Data Access and Sharing: NEF facilitates secure access to subscriber data and network context information (e.g., location, session status) for authorized applications and services, enabling personalized and context-aware service delivery.

4. Service Orchestration: NEF supports service orchestration by coordinating interactions between multiple network functions and external applications/services. It enables dynamic service composition and delivery based on real-time network conditions and user preferences.

5. Billing and Charging Integration: NEF interacts with charging systems to provide usage data and facilitate accurate billing and charging processes for services accessed through third-party applications.

6. Network Slicing Support: NEF supports network slicing by enabling

the exposure of network slice-specific capabilities and services to authorized tenants or service providers. This allows for tailored service offerings and resource allocations within a network slice environment.

7.SMF (Service Management Function): NEF interacts with SMF to expose session management capabilities and QoS policies, allowing third-party applications to request and manage data sessions.

8. PCF (Policy Control Function): NEF coordinates with PCF to expose policy rules and QoS parameters, enabling external applications to request specific service levels and traffic handling policies.

9. AMF (Access and Mobility Management Function): NEF interacts with AMF to expose access control policies and subscriber authentication mechanisms, ensuring secure access to network services.

10. UPF (User Plane Function): NEF may expose data forwarding and traffic steering capabilities of UPF to optimize data delivery paths based on application requirements.

6. NRF->

NRF stands for Network Repository Function. It serves as a centralized repository for network functions and their capabilities within the 5G Core (5GC) architecture.It acts as a centralized database or registry that stores information about available network functions, their capabilities, and their current operational status.

Funtionality->
Function Discovery: NRF facilitates the discovery of network functions (NFs) and their associated capabilities within the 5G network.

Service Discovery: It enables the discovery of network services that can be accessed or utilized by other network functions, applications, or

services.

Capability Exposure: NRF exposes the capabilities and characteristics of network functions to other components in the 5GC, such as Service Management Function (SMF), Access and Mobility Management Function (AMF), and others.

Network Slice Support: NRF supports network slicing by maintaining information about the network functions and capabilities available within each network slice. This enables efficient management and orchestration of slice-specific resources and services.

Dynamic Updates: NRF supports dynamic updates of NF capabilities and status, ensuring that the network functions are always aware of the latest available resources and configurations.

Fault Management: NRF plays a role in fault management by providing information about the operational status of network functions. This helps in network troubleshooting and fault recovery processes

Service Management Function (SMF): NRF provides SMF with information about available UPF (User Plane Function) instances and their capabilities to facilitate session management and traffic handling.

Policy Control Function (PCF): NRF provides PCF with information about QoS policies, charging rules, and other policy-related capabilities to enforce policy decisions.

AMF (Access and Mobility Management Function): NRF provides AMF with information about available access technologies and authentication methods to manage user access and mobility.

UDM (Unified Data Management): NRF interacts with UDM to exchange

subscriber-related information and manage subscriber data.

7. UDM->

UDM is a core network function in the 5G Core Network (5GC) that centralizes the management of subscriber-related data and authentication information.
It replaces the Home Subscriber Server (HSS) used in previous generations (like 4G/LTE) and extends its capabilities to support the diverse requirements of 5G services.

Funtionality->

Subscriber Data Management:

UDM stores and manages subscriber profiles, including subscription information, service preferences, authorized services, and QoS (Quality of Service) profiles.
It provides a centralized repository for maintaining up-to-date subscriber information, ensuring consistency across the network.

Authentication and Authorization:

UDM manages authentication credentials (such as authentication vectors) used for secure access to the 5G network.
It supports authentication methods like 5G AKA (Authentication and Key Agreement) to verify the identity of subscribers and authorize network access.
Subscription Management:

UDM handles subscription management, including provisioning and de-provisioning of services for subscribers.
It supports flexible subscription models and service configurations to accommodate various service plans and offerings.
Policy Enforcement:

UDM provides subscriber-related data to other network functions, such as Policy Control Function (PCF) and Access and Mobility Management Function (AMF), to enforce policies related to QoS, charging, and service entitlements.
Network Slicing Support:

UDM supports network slicing by managing subscriber profiles and service subscriptions specific to each network slice.
It enables personalized service delivery and resource allocation within a sliced network environment.
Integration with Authentication Functions:

UDM interacts with the Authentication Server Function (AUSF) to authenticate subscribers using authentication vectors and ensure secure access to the network.

Interaction with other component->
AMF (Access and Mobility Management Function): UDM provides subscriber data to AMF for access control and mobility management.

SMF (Service Management Function): UDM supplies subscriber QoS profiles and service entitlements to SMF for session management and traffic handling.

PCF (Policy Control Function): UDM provides subscriber-related data to PCF for policy enforcement related to QoS and charging.

8. AUSF->

5G AUSF receives authentication requests from the Access and Mobility Management Function (AMF) and interacts with Unified Data Management (UDM) to obtain authentication vectors for processing 5G AKA authentication, and validates network responses to determine whether or not the authentication was successful.

Function of AUSF:

Authentication: When a subscriber tries to access the 5G network, the AUSF performs authentication by verifying the subscriber's identity and checking whether they have the proper credentials to access the network.

Authorization: After authentication, the AUSF performs authorization by checking whether the subscriber has the appropriate authorization to access specific network functions or services.

Security context: The AUSF determines the appropriate security context for the subscriber based on their identity, subscription data, and authorization level.

Mobility management: The AUSF interacts with other network functions, such as the Access and Mobility Management Function (AMF), to manage subscriber mobility and handover procedures.

Session management: The AUSF supports session management, including the establishment, maintenance, and termination of 5G network sessions.

Subscriber data management: The AUSF interacts with the Unified Data Management (UDM) function to manage subscriber data and profiles

9. N3IWF ->

N3IWF is a key component within the 5G Core Network (5GC) architecture, specifically designed to enable interworking between 5G networks and non-3GPP access networks.

It acts as an interface or gateway that allows devices connected via non-3GPP access technologies (like Wi-Fi) to access 5G core network services and functionalities.

Key Functionalities:

Access Interworking: N3IWF enables devices using non-3GPP access technologies (e.g., Wi-Fi, Ethernet) to establish connectivity with the 5G core network.

Bearer Management: It manages the establishment, modification, and termination of bearers (logical connections) between the non-3GPP access network and the 5G core network.

Session Management: N3IWF handles the setup and release of sessions for devices accessing the 5G network via non-3GPP access technologies, ensuring seamless connectivity and session continuity.

IP Address Allocation: It may perform IP address allocation and management for devices connected through non-3GPP access, ensuring proper addressing within the 5G network architecture.

Security Functions: N3IWF incorporates security functions to protect data and communications between devices and the 5G core network, including authentication, encryption, and integrity protection.

Policy Enforcement: It enforces policies related to traffic management, quality of service (QoS), and access control for devices using non-3GPP access technologies, ensuring adherence to operator-defined rules and service agreements.

Mobility Support: N3IWF supports seamless mobility management for devices moving between different non-3GPP access points or between

non-3GPP and 3GPP access networks.

Enhanced Coverage and Capacity: N3IWF enables operators to extend 5G network coverage and capacity by leveraging existing non-3GPP access technologies.

Offload and Load Balancing: It supports offloading of data traffic from 5G radio access networks (RANs) to Wi-Fi or Ethernet networks, optimizing network resources and improving user experience.

Multi-access Connectivity: N3IWF facilitates seamless connectivity for devices that can utilize both 5G and non-3GPP access technologies, providing flexibility and continuity of service.

10. NSSF-->

NSSF is a crucial component in 5G networks responsible for selecting appropriate network slices for user equipment (UE) based on specific requirements and policies.

Functionality-->

1. Network Slicing Management: NSSF plays a key role in managing and orchestrating network slices. Network slicing allows the creation of multiple virtual networks (slices) on top of a shared physical infrastructure, each tailored to different use cases.

2. Slice Selection: When a UE initiates a session or communication, NSSF determines the best-suited network slice based on factors like the UE's service requirements (e.g., latency, bandwidth), network conditions, and operator policies.

3. Dynamic Adaptation: NSSF supports dynamic adaptation of network slices based on real-time conditions and user demands. This

flexibility ensures optimal resource allocation and efficient use of network resources.

4. Deployment: NSSF is typically deployed as part of the Service Based Architecture (SBA) in 5G networks, ensuring scalability, flexibility, and efficient management of network resources across diverse use cases.

11. AF (Application Function)-->

AF is a key component in 5G networks responsible for interacting with applications and services running over the network. It plays a crucial role in managing and controlling the behavior of specific applications based on policies and service requirements.

Functionality->

1. Application Awareness: AF is aware of the characteristics and requirements of different applications and services. It can distinguish between various types of traffic

2. Policy Enforcement: AF enforces policies defined by network operators or service providers. These policies can dictate parameters such as prioritization, bandwidth allocation, latency requirements, and access control for specific applications.

3. Traffic Steering: AF can steer traffic to specific network slices optimized for different types of applications. For example, latency-sensitive applications may be directed to slices with ultra-low latency characteristics, while high-throughput applications may use slices with high bandwidth.

4. Service Orchestration: AF participates in the orchestration of network resources and services. It interacts with other network

functions such as the Session Management Function (SMF) and Network Slice Selection Function (NSSF) to ensure that the network resources are allocated efficiently according to application requirements.

12. EASDF-->

EASDF is an evolved version of the Access and Mobility Management Function (AMF) in 5G networks. It enhances the capabilities of AMF to manage and control access to the 5G network and facilitate seamless mobility for user equipment (UE).

Functionality-->

1. Access Control
2. Mobility Management
3. Session Management
4. Policy Enforcement

13. NSSF-->

NSSF is a core network function in 5G architecture responsible for selecting and controlling network slices based on the requirements of user equipment (UE) and applications.

Functionality-->

1. Network Slicing Management: NSSF manages and orchestrates network slices, which are virtualized end-to-end networks customized for specific services or applications.

2. Slice Selection: When a UE initiates a session, NSSF determines the appropriate network slice to allocate based on factors like service type, quality of service (QoS) requirements, and operator policies.

3. Policy Enforcement: NSSF enforces policies defined by the network operator regarding slice selection, ensuring that resources are allocated efficiently and according to service level agreements (SLAs).

14. SCP-->

SCP is a key component in 5G networks that provides a standardized interface for exposing and managing network services and capabilities. It enables third-party applications and services to interact with and utilize network functions and resources.

Functionality:

Service Exposure: SCP exposes a catalog of network services and capabilities available within the 5G network. This includes functionalities such as network slicing, Quality of Service (QoS) parameters, authentication services, and more.

API Management: SCP provides standardized APIs (Application Programming Interfaces) that allow external applications and services to discover, request, and utilize network capabilities. These APIs facilitate integration with the 5G network and enable service innovation.

Policy Enforcement: SCP enforces policies related to service access and usage. It ensures that third-party applications adhere to security, privacy, and operational policies defined by the network operator.

Service Orchestration: SCP plays a role in orchestrating network services and resources in response to service requests from external applications. It coordinates with other network functions to ensure efficient allocation and utilization of resources.

Billing and Charging: SCP may also handle aspects related to billing and charging for services consumed by third-party applications, ensuring that usage is accurately accounted for and billed according to predefined models.

Security and Authentication: SCP includes security mechanisms to authenticate and authorize access for external applications. It ensures secure interactions between third-party services and the network infrastructure.

15. NSACF-->

NSACF verifies the identity of entities (such as user equipment, applications, or services) requesting access to specific network slices. It ensures that only authenticated entities can access the resources allocated to a particular slice.

Functionality-->

1.Authorization: NSACF determines whether an authenticated entity has permission to access a specific network slice based on predefined policies and rules.

2. Policy Enforcement: NSACF enforces policies related to slice access and usage. These policies can include Quality of Service (QoS) requirements, security parameters.

3. Dynamic Management: NSACF supports dynamic management of authentication and authorization policies based on real-time conditions and changes in network slice configurations.

4. Integration with Network Slicing: NSACF interfaces with other network functions involved in network slicing, such as the Network Slice Selection Function (NSSF) and the Policy Control Function (PCF).

16. RAN (Radio Access Network)->

RAN is the part of the telecommunications system that connects user devices (such as smartphones, tablets, IoT devices) to the core network via wireless links.

Functionality:

1. Radio Transmission: RAN manages the radio transmission and reception between user equipment (UE) and base stations.

2. Radio Resource Management: RAN optimizes the allocation and utilization of radio resources (such as frequencies, bandwidth, and power) to ensure efficient communication for all connected devices.

3. Latency Management: RAN plays a crucial role in minimizing latency by reducing the time it takes for data to travel between UE and the core network.

17. UE (User Equipment)->

UE encompasses a wide range of devices that connect to 5G networks to access various services and applications. These devices include smartphones, tablets, laptops, IoT devices, and other gadgets capable of wireless communication.

Functionality:

Wireless Connectivity: UE uses radio interfaces such as 5G New Radio (NR), LTE, and Wi-Fi to connect to the network and communicate with other devices and services.

Multimedia Capabilities: Modern UE devices support multimedia applications such as video streaming, online gaming, video conferencing, and high-definition content consumption over 5G

networks, leveraging the increased bandwidth and lower latency.

Enhanced Mobile Broadband (eMBB): UE in 5G networks benefits from higher data rates and improved network capacity, enabling faster downloads, smoother streaming, and better overall user experience compared to previous generations of mobile networks.

18. Data Network->

Data Network (DN) refers to the core network that handles all data traffic. It includes various components like the User Plane Function (UPF), Session Management Function (SMF), and Access and Mobility Management Function (AMF). The DN is responsible for routing data packets between the user equipment (UE) and external networks or services.