**PDCP (Packet Data Convergence Protocol) process**

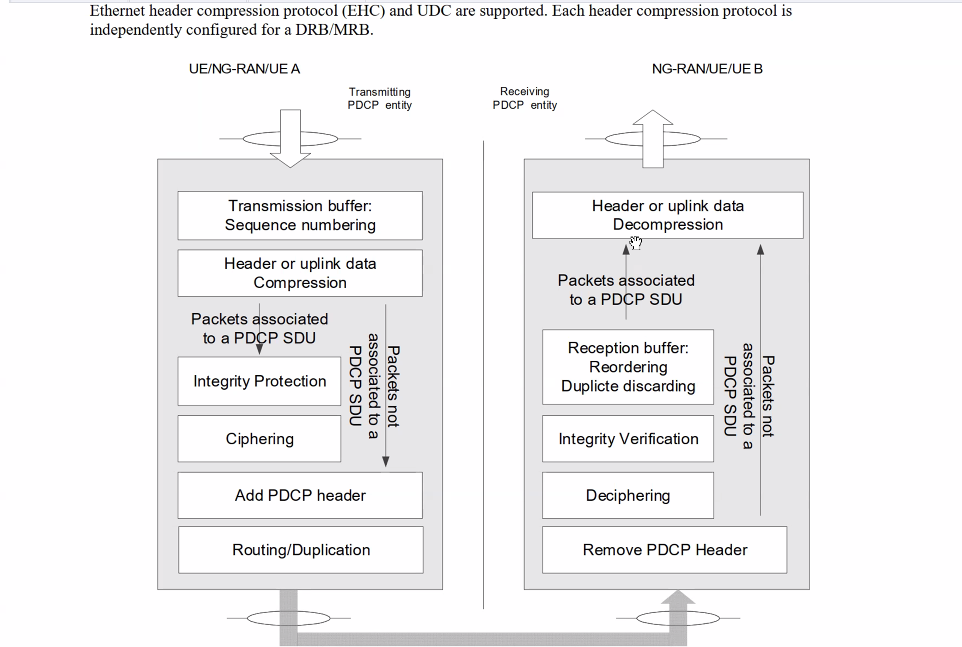
**PDCP (Packet Data Convergence Protocol) process** in a 5G network, explaining how data is processed before transmission and after reception.

**Think of PDCP as a Postal System for Data Packets**

Imagine sending a **package** (data) from **Person A (UE/NG-RAN)** to **Person B (NG-RAN/UE)** via a courier service. The steps are:

**At the Sender's Side (UE/NG-RAN/UE A - Transmitting PDCP Entity)**

1. **Labeling the Package (Sequence Numbering)** – Each data packet gets a unique number so that it can be tracked and delivered in order.
2. **Compressing the Package (Header Compression)** – To save space and speed up delivery, unnecessary information (extra weight) is removed.
3. **Securing the Package (Integrity Protection & Ciphering)** – The package is sealed and locked to ensure no one tampers with it during transit.
4. **Adding a Tracking Label (PDCP Header)** – A label is attached to help identify and process the packet at the receiver's end.
5. **Sending the Package (Routing/Duplication)** – The packet is sent via the best available route.



**At the Receiver's Side (NG-RAN/UE/UE B - Receiving PDCP Entity) (Bottom to Top)**

1. **Removing Extra Labels (Remove PDCP Header)** – The tracking label is removed, and the data is ready to be used.
2. **Unlocking the Package (Deciphering)** – The locked data is decrypted to make it readable.
3. **Checking the Seal (Integrity Verification)** – Confirms the data is authentic and not tampered with.
4. **Sorting & Removing Duplicates (Reordering & Duplicate Discarding)** – Ensures packets arrive in the correct order, and duplicates are removed.
5. **Uncompressing the Package (Header Decompression)** – The compressed data is restored.

**PDU (Protocol Data Unit)**

* A **unit of data** exchanged between layers in a network.
* Different types: **SDU (Service Data Unit), PDCP PDU, RLC PDU, MAC PDU, etc.**
* Example: **IP packet in the network layer, MAC frame in the data link layer.**

**PDCP (Packet Data Convergence Protocol)**

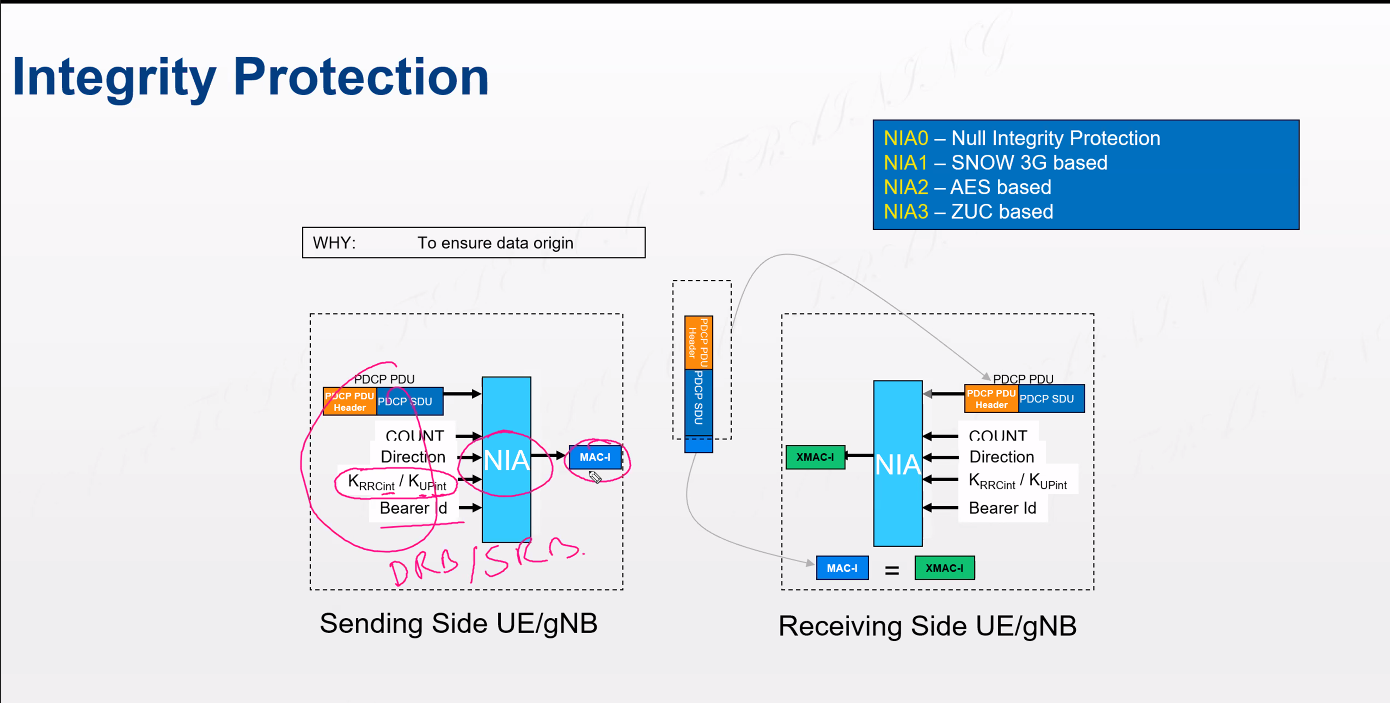
* A **layer in 5G NR and LTE** that sits above RLC (Radio Link Control).
* Functions:
  1. **Header Compression/Decompression** (e.g., ROHC for efficient transmission).
  2. **Integrity Protection & Verification** (for control plane security).
  3. **Ciphering & Deciphering** (for data confidentiality).
  4. **Sequence Numbering & Reordering** (for in-order delivery).
  5. **Duplication Handling** (for robust transmission in dual connectivity).

**Integrity Protection**

**Integrity Protection** is like a security seal for your data. Imagine you send a letter in a sealed envelope. The seal ensures that no one has opened or changed the letter before it reaches the person you sent it to.

In the world of technology, especially in networks like 5G, **Integrity Protection** does the same thing for your data. It makes sure that the information sent from one device to another hasn’t been tampered with or altered during transmission. It’s like a digital "seal" that guarantees the data is exactly what was sent and hasn’t been messed with along the way.

1. **Purpose of Integrity Protection**:
   * **Why**: Ensures data origin authenticity and integrity.
   * **Real-life Correlation**: Similar to how a sealed envelope ensures that a letter has not been opened or altered before reaching the recipient.
2. **Components Mentioned**:
   * **POCP POU/BDU**: These likely refer to protocol entities or functions within the network.
   * **COUNIT**: Could be a unit or module responsible for certain operations.
   * **Direction**: Indicates the flow of data (uplink or downlink).
   * **Kpacur / Kupin**: These might be keys used for encryption and integrity protection.
   * **Bearer id**: Identifies the specific data bearer or channel.
3. **Integrity Algorithms (NIA)**:
   * **NIA0 – Null Integrity Protection**: No integrity protection is applied.
   * **NIA1 – SNOW 3G based**: Uses the SNOW 3G algorithm.
   * **NIA2 – AES based**: Uses the AES algorithm.
   * **NIA3 – ZUC based**: Uses the ZUC algorithm.
   * **Real-life Correlation**: Similar to different types of locks (basic to advanced) used to secure doors, with varying levels of security.
4. **Sending and Receiving Sides**:
   * **Sending Side (UE/gNB)**: The user equipment (UE) or base station (gNB) that sends data.
   * **Receiving Side (UE/gNB)**: The UE or gNB that receives data.
   * **Real-life Correlation**: Like a postal system where a sender mails a letter, and the recipient receives it, ensuring it hasn't been tampered with.
5. **MAC (Message Authentication Code)**:
   * **MAC1, MAC2, MAC3**: These are likely different types of MACs used to verify data integrity.
   * **Real-life Correlation**: Similar to checksums or digital signatures that verify the authenticity of software downloads.
6. **Flow**:
   * Data is sent from the sending side with integrity protection applied using one of the NIA algorithms.
   * The receiving side verifies the integrity using the corresponding MAC.
   * **Real-life Correlation**: Like sending a tamper-evident package; the recipient checks the seal to ensure it hasn't been opened.



**1. User Equipment (UE) – The Device (Smartphone, IoT, etc.)**

📱 **Real-life analogy:** Think of the UE as a smartphone or IoT device that connects to the network to access data and services.

* Uses **N1 Interface** to communicate with **AMF**.
* Defined by **TS 24.501**.

**2. (R)AN – The Access Point (5G Towers, Base Stations, gNB)**

📡 **Real-life analogy:** Similar to a WiFi router that connects your phone to the internet, (R)AN (Radio Access Network) provides wireless connectivity.

* Uses **N2 Interface** to communicate with **AMF**.
* Defined by **TS 38.413**.

**3. AMF (Access & Mobility Management Function) – The Traffic Controller**

🚦 **Real-life analogy:** AMF acts like an air traffic controller, managing device registrations and mobility (handover between towers).

* Handles authentication requests, handovers, and paging.
* Communicates with **UE via N1**, **RAN via N2**, and **AUSF for authentication**.
* Defined by **TS 29.509**.

**4. AUSF (Authentication Server Function) – The Security Guard**

🔐 **Real-life analogy:** Just like a bank verifies your identity before giving access to your account, AUSF verifies if the UE is authorized to use the network.

* Uses **Nausf Interface** to authenticate users.
* Works with **UDM (User Data Management)** to validate subscriber identity.
* Defined by **TS 29.509**.

**5. UDM (Unified Data Management) – The Identity Vault**

📂 **Real-life analogy:** UDM is like a passport database that stores all necessary details about users for authentication and access authorization.

* Communicates with **AMF and AUSF** for identity verification.
* Defined by **TS 29.503**.

**6. SMF (Session Management Function) – The Internet Manager**

🌍 **Real-life analogy:** SMF is like your internet service provider (ISP), managing data sessions, IP addresses, and quality of service (QoS).

* Works with **AMF** via **N11 Interface** to set up data sessions.
* Communicates with **UPF (User Plane Function)** for data forwarding.
* Defined by **TS 29.518**.

**7. UPF (User Plane Function) – The Internet Router**

🔀 **Real-life analogy:** UPF is like a home router, forwarding data between the internet and devices.

* Receives session setup from **SMF** and routes actual data packets.
* Uses **N6 Interface** to connect to the **Data Network (DN)** (e.g., the Internet).
* Defined by **TS 29.281**.

**8. PCF (Policy Control Function) – The Network Rule Enforcer**

📜 **Real-life analogy:** PCF is like a traffic police system that ensures fair use of network resources (e.g., limiting speed after data cap is reached).

* Works with **SMF** to apply policies and QoS rules.
* Defined by **TS 29.510**.

**9. NEF, NRF, NSSF – The Service & Resource Managers**

🏢 **Real-life analogy:**

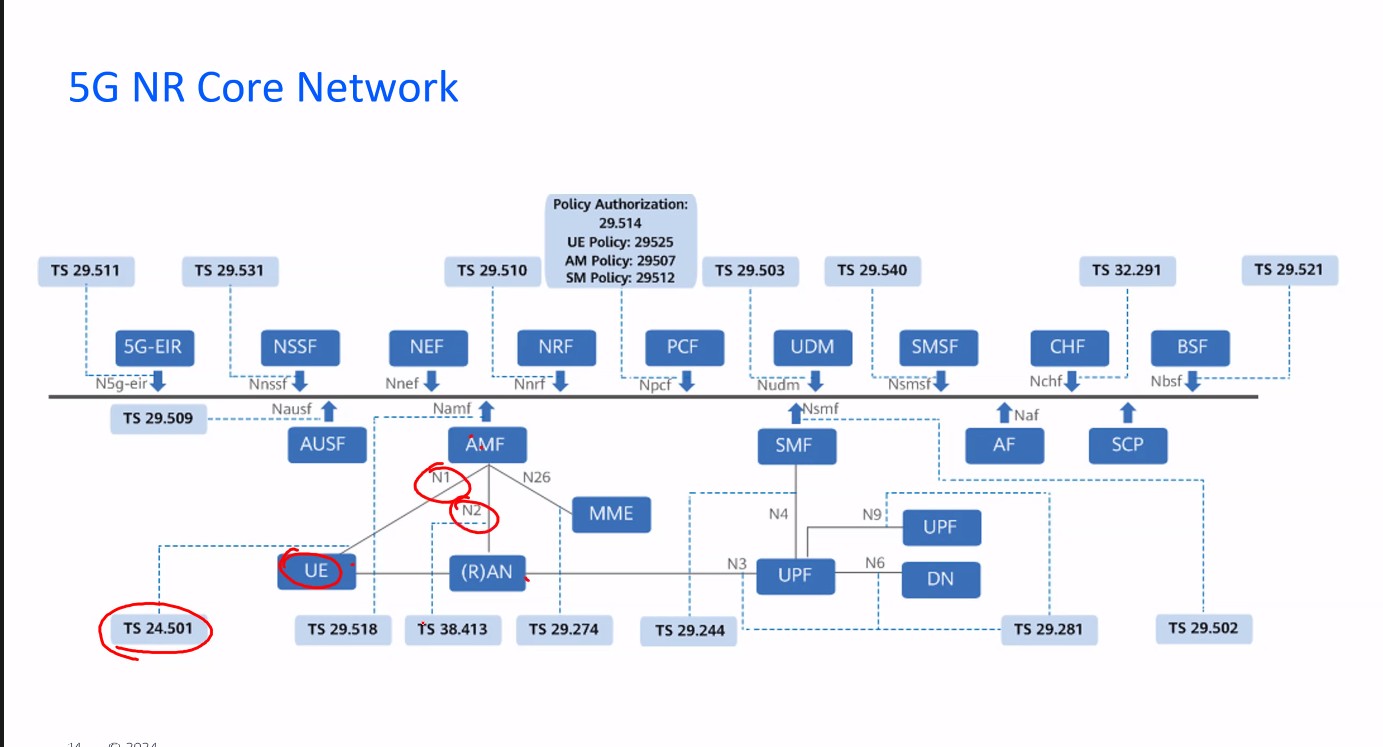
* **NEF (Network Exposure Function):** Like an API gateway, allowing external applications to interact with the core network.
* **NRF (Network Repository Function):** Like a phone directory, keeping track of network functions.
* **NSSF (Network Slice Selection Function):** Like a VIP lounge system, assigning users to network slices based on service needs.

**Conclusion – The 5G Core Works Like a Digital City**

Imagine the 5G Core Network as a **smart city** where:

* **UE** is a person traveling in the city.
* **RAN** is the city’s metro station.
* **AMF** is the central control station managing mobility.
* **AUSF & UDM** are ID verification checkpoints.
* **SMF & UPF** are highways and internet providers.
* **PCF & NSSF** ensure smooth traffic and quality service.

Each part plays a **crucial role in ensuring seamless, secure, and high-speed 5G connectivity**!



**4. Security** (TS 33.501)

 **SEAF (Security Anchor Function)** – The Gatekeeper

 **AUSF (Authentication Server Function)** – The Security Guard

 **UDM (Unified Data Management)** – The Database Keeper

 **SCP (Service Communication Proxy)** – The Message Dispatcher

**3. PCC Architecture** (TS 23.503)

**2. System Architecture** (TS 23.501)

**1. NG-RAN (Radio Access Network)**

 **AMF (Access & Mobility Management Function)** – The Traffic Controller

 **SMF (Session Management Function)** – The Session Manager

 **UPF (User Plane Function)** – The Data Router

 **NRF (Network Repository Function)** – The Directory Manager

 **PCF (Policy Control Function)** – The Rule Enforcer

 **AF (Application Function)** – The Service Provider

 **NWDAF (Network Data Analytics Function)** – The Network Analyzer

 **CHF (Charging Function)** – The Billing Manager

 **UE (User Equipment)** – Mobile Devices, IoT Devices

 **(R)AN (Radio Access Network)** – 5G Towers, Base Stations, gNB

**Understanding AMF in 5G (Real-Life Correlation & Sequence)**

**AMF is like a traffic controller in a smart city, ensuring efficient and secure communication between users and the 5G core network.**

**1. User Equipment (UE) – The Passenger 🚶‍♂️📱**

* **The UE (mobile phone, IoT device, etc.) is like a passenger in a city.**
* **It connects to the 5G network through N1: NAS (Non-Access Stratum) Interface.**
* **The device can be in Idle or Connected mode, like a passenger waiting or actively traveling.**

**2. RAN (gNB) – The Metro/Bus Station 🚉🚏**

* **The gNB (Next-Generation Node B) acts like a bus or metro station, linking passengers (UE) to the core network.**
* **It connects to AMF using N2: NGAP (Next-Generation Application Protocol).**
* **It handles handover, like when a passenger switches between metro lines without losing connectivity.**

**3. AMF – The Traffic Controller 🚦🕵️‍♂️**

* **AMF (Access and Mobility Management Function) is like a traffic controller, ensuring smooth movement of users.**
* **It manages registration, authentication, paging, and mobility.**
* **It decides which roads (network slices) a passenger should take for an optimized journey.**

**4. NAS Procedures – The ID Check & Security 🔐👮‍♂️**

* **Just like checking tickets and IDs at an airport, NAS (Non-Access Stratum) procedures handle:**
  + **Authentication & Security (to verify users).**
  + **Identity & Configuration Update (ensuring users get proper network settings).**
  + **Paging & Service Requests (allowing calls, messages, and data).**

**5. NGAP Procedures – Managing Traffic Flow 🚦🚗**

* **Just like a smart traffic system, NGAP (Next-Generation Application Protocol) helps in:**
  + **Handover (XN/N2-based) – Ensuring a smooth transition when moving between cities (network cells).**
  + **Path Switching – Redirecting traffic for better service.**
  + **Session Resource Setup – Allocating network resources.**

**6. Security Features – Surveillance & Encryption 🔒🔍**

* **Like CCTV cameras & encryption locks, security features include:**
  + **Integrity Protection & Ciphering – Preventing eavesdropping.**
  + **Key Management (K\_AMF) – Secure key exchange between devices.**

**7. SMF (Session Management Function) – The Toll Booth 🚧💳**

* **SMF manages sessions and QoS (Quality of Service) like a toll booth ensuring VIP lanes for premium users.**

**8. AUSF (Authentication Server Function) – Immigration Check 🛂🆔**

* **AUSF ensures authentication like an immigration officer verifying travelers before allowing them into a country.**

**9. UDM (Unified Data Management) – The Government Database 🗃📜**

* **UDM stores user subscriptions and access authorizations, similar to a national ID database.**

