Wi-Fi in Public Networks / IP Multimedia Subsystem

Comunicações Móveis

DETI – UA

Outubro 2024

Wi-Fi in Public Scenarios

Public Wi-Fi → HotSpots

- Convenient, seemingly open Wi-Fi networks
- Pros
  - Free
  - In comercial áreas
- Cons
  - What are they doing with our traffic?
  - Risky
    - Main-in-the-middle attacks
    - Packet sniffing
    - Malicious hotspots
- Remedies
  - VPN

Public Wi-Fi → HotSpots

- Convenient
- Pros
  - Free
  - In comerc
- Cons
  - What are
  - Risky
    - Main-i
    - Packet
    - Malici
- Remedies
  - VPN

Users can be malicious too!
How can we protect things from the network side?

Captive Portals

- What is a Captive Portal?
  - A Captive Portal is a web page displayed to users when they attempt to access the internet over WLAN (Wi-Fi), typically in public networks (airports, cafes, universities).
  - Purpose: Controls access by requiring authentication or acceptance of terms before granting network access.
- Why Captive Portals?
  - Security: Controls unauthorized access.
  - Monetization: Charges for usage or captures user data.Usage Tracking: Records user activity or limits bandwidth.

How a Captive Portal Works

- Workflow Overview:
  - User connects to the Wi-Fi network.
  - Any HTTP request is intercepted and redirected to the Captive Portal.
  - User interacts with the portal (login, payment, acceptance of terms).
  - Upon success, the user is granted access to the internet.

Technical Components

- DHCP and DNS:
  - DHCP (Dynamic Host Configuration Protocol): Assigns IP addresses to users.
  - DNS (Domain Name System): The Captive Portal intercepts the initial DNS requests and redirects them to the login page.
- Firewall Rules:
  - Filters traffic to allow only HTTP/HTTPS access to the Captive Portal until authentication is complete.
- Authentication Server:
  - May be based on RADIUS or LDAP, authenticating user credentials and enabling access.

Network Redirection in Captive Portals

- Redirection Mechanism:
  - Upon connection, web requests are intercepted and the user is automatically redirected to the portal.
  - Usually, a DNS hijacking or HTTP interception mechanism is employed to force this redirect.
- DNS-Based vs. HTTP-Based:
  - DNS-based: Captive Portal DNS server gives an incorrect IP address to all external queries.
  - HTTP-based: HTTP traffic is intercepted, redirecting any web request to the login page.

Authentication and Authorization

- Types of Authentication:
  - Open System: Just accept terms (common in cafes and airports).
  - Voucher System: Use prepaid codes for access (common in hotels).
  - Username/Password: Secure login via captive portal (common in educational institutions).
  - Social Media Login: Some portals allow login via Facebook, Google, etc.
- Authorization:
  - Based on successful authentication, the portal assigns a firewall rule that allows full internet access.

Use Cases

- Public Wi-Fi (Airports, Cafes):
  - Open portals that require terms of service acceptance.
- Universities/Schools:
  - Secure login via credentials, controlling student access.
- Enterprises:
  - Employee and guest network separation using different login methods.
- Hotels:
  - Voucher or paid login systems to control bandwidth and usage.

Security Considerations

- Vulnerabilities:
  - Susceptibility to Man-in-the-Middle (MitM) attacks.
  - Weak SSL/TLS certificates can expose user credentials.
  - Users bypassing portals using VPN or spoofing DNS.
- Countermeasures:
  - Enforcing HTTPS redirects.
  - Implementing strong encryption (TLS).
  - Capturing traffic before granting full access.

Limitations

- User Experience:
  - Some devices (IoT, gaming consoles) struggle with captive portals.
  - Captive portals may not work well with encrypted DNS (DoH/DoT).
- Performance Issues:
  - Redirection and login pages may slow down connection times.
  - Users could experience inconsistent internet connectivity.

Captive Portal in Modern Networks

- Integration with Hotspot 2.0:
  - Hotspot 2.0 allows automatic, secure Wi-Fi connection without needing captive portals.
  - Focus is shifting to seamless user experience through Wi-Fi Passpoint instead of captive portal interruptions.
- Emerging Alternatives:
  - MAC address authentication or certificate-based access.
  - Moving toward more secure and frictionless network access methods.

IMS

IP-Multimedia Subsystem

Remember SIP – Session Initiation Protocol

- Signalling protocol used for establishing real-time Communications sessions over IP networks
  - Voice, vídeo, messaging, …
- SDP – Session Description protocol – used for describing multimedia Communications sessions
  - How and where to transmit media
    - Media type: áudio, vídeo, text, etc
    - Codec: h.264 for vídeo, G.711 for áudio, agmonst many others
    - Media transport: IP address and port numbers
    - Session timing
- RTP – Real-time Transport Protocol
  - Used for the actual transmission of real-time auidio, vídeo and other multimedia
- RTCP – RTP Control Protocol
  - Used to monitor transmission quality

MGCP – Media Gateway Control Protocol

- Controls media gateways in VoIP networks
- Bridge IP-based IMS networks and traditional circuit-switched networks (i.e., interworking)

IMS

- Service framework to deliver multimedia/interactive services over IP Networks
  - Voice
  - IP Centrex Service
  - Video chat/conferencing
  - Instant Messaging-like multimedia services
    - VoNR (Voice-over New Radio)
    - VoLTE (Voice-over Long Term Evolution)
    - VoWiFi (Voice-over WiFi)
    - RCS (Rich Communications Service)

IMS - IP Multimedia Service

Principles

- QoS characteristics differentiation for voice or video associated with a multimedia session (streaming, IM, etc.)
- Separation of the planes IP data and session control (SIP)
- Independant from the access network

R5

IMS for mobile networks GPRS, EDGE, UMTS & CDMA2000
Non real time services
IP multimedia applications plate-form
IETF specifications based

R6

IMS extended to wideband fixed networks (xDSL, WLAN, cable, ...)

Supports services convergence on fixed and mobile networks (conversion CS voice traffic in IP)

Advantages

- Introduction of multimedia services with QoS management
- Integration with other networks (WLANs, fixed, CDMA2000, ...)
- Flexible billing: billing / service, connectivity, QoS, time, destination

Drawbacks

- Implementation of many equipments, softwares, interfaces, protocols, which may cause integration, interworking and optimisation problems
  - Ex.: S-CSCF (*Call Status Control Function*); SIP AS (*SIP Application Server*); OSA SCS (*Service Capability Server*); IM-SSF (*Inter-working Module*); CSE (*Camel Service Environment*); HSS *(Home Subscriber Server)*
- Security and QoS with Internet interconnection

IMS – Key Architectural Principals

- Border Functions
  - Access and Network Border Security
  - QoS and Admission Control
  - Media and Signaling Adaptation
- Core Functions
  - Subscriber Management – Registration
  - Session Switching – Set-up and tear-down of session legs, Session state maintenance, Application Server invocation
  - Session Routing – Breakout to external networks
  - Centralized Provisioning – Subscriber and Routing data
- Application Functions
  - Access to legacy applications
  - Native SIP Applications
  - Service Brokering

SIP Protocol

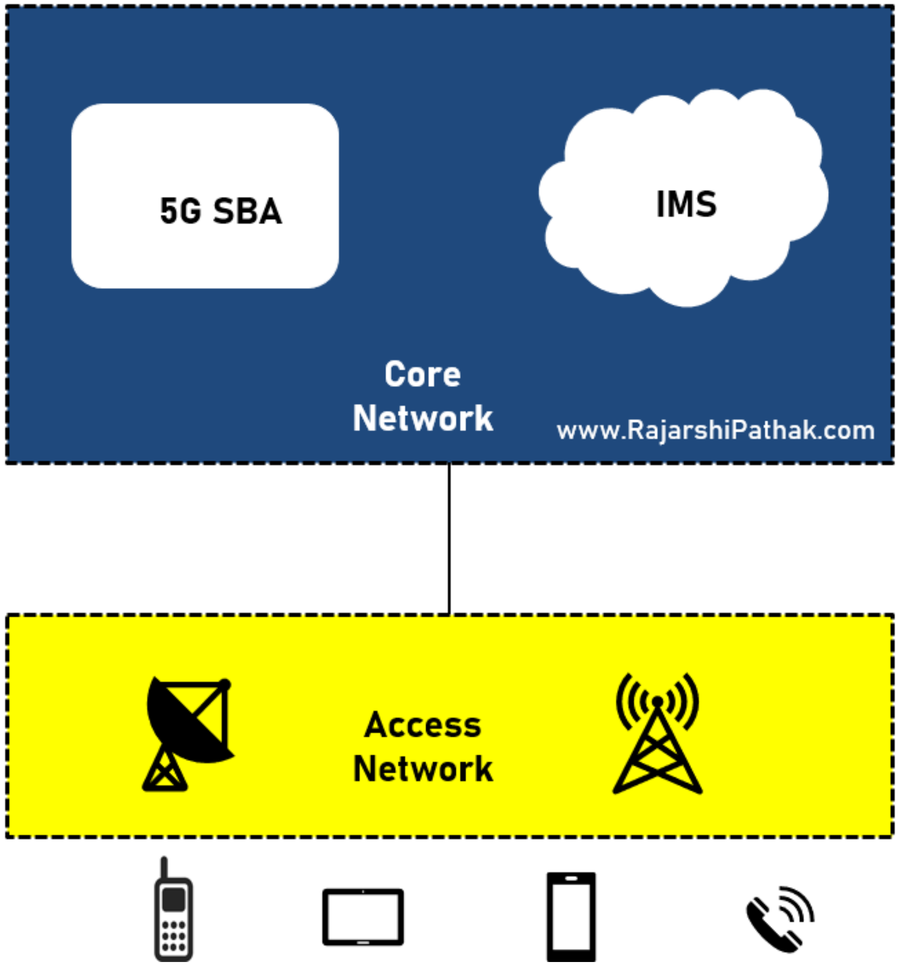
- Defined in IETF RFC 3261
  - "… an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences."
- SIP is to the Internet what SS#7 is to telephony
- In IMS, SIP is extended to include extra functionality
  - E.g. 3GPP TS 23.228
- At the core of IMS there are several SIP proxies:
  - I-CSCF, S-CSCF, P-CSCF
  - The Call Session Control function (CSCF) is the heart of the IMS architecture
  - The main functions of the CSCF:
    - provide session control for terminals and applications using the IMS network
    - secure routing of the SIP messages,
    - subsequent monitoring of the SIP sessions and communicating with the policy architecture to support media authorization.
    - responsibility for interacting with the HSS.

Services in IMS

- IMS is an advanced infrastructure enabling services. But the services are in the end points or peers (calls, etc.), not in the IMS
- Application Servers (AS) are the key part to endow IMS with services
- AS are not owned by the network operator
  - (therefore not part of IMS)
- AS offered services enjoy all IMS advantages
- AS interact – using SIP - with the S-CSCF (which controls user's SIP session)
- AS can behave as another SIP proxy or as a SIP UA (terminal)
  - in this case they also receive and send media!

Where is IMS?

- IMS is access independente
- In 5G, it connects to the 5G SBA (Service-based Architecture) and it delivers
  - Voice over 5G (VoNR or Vo5G)
  - Allows roaming features over 5G/4G networks

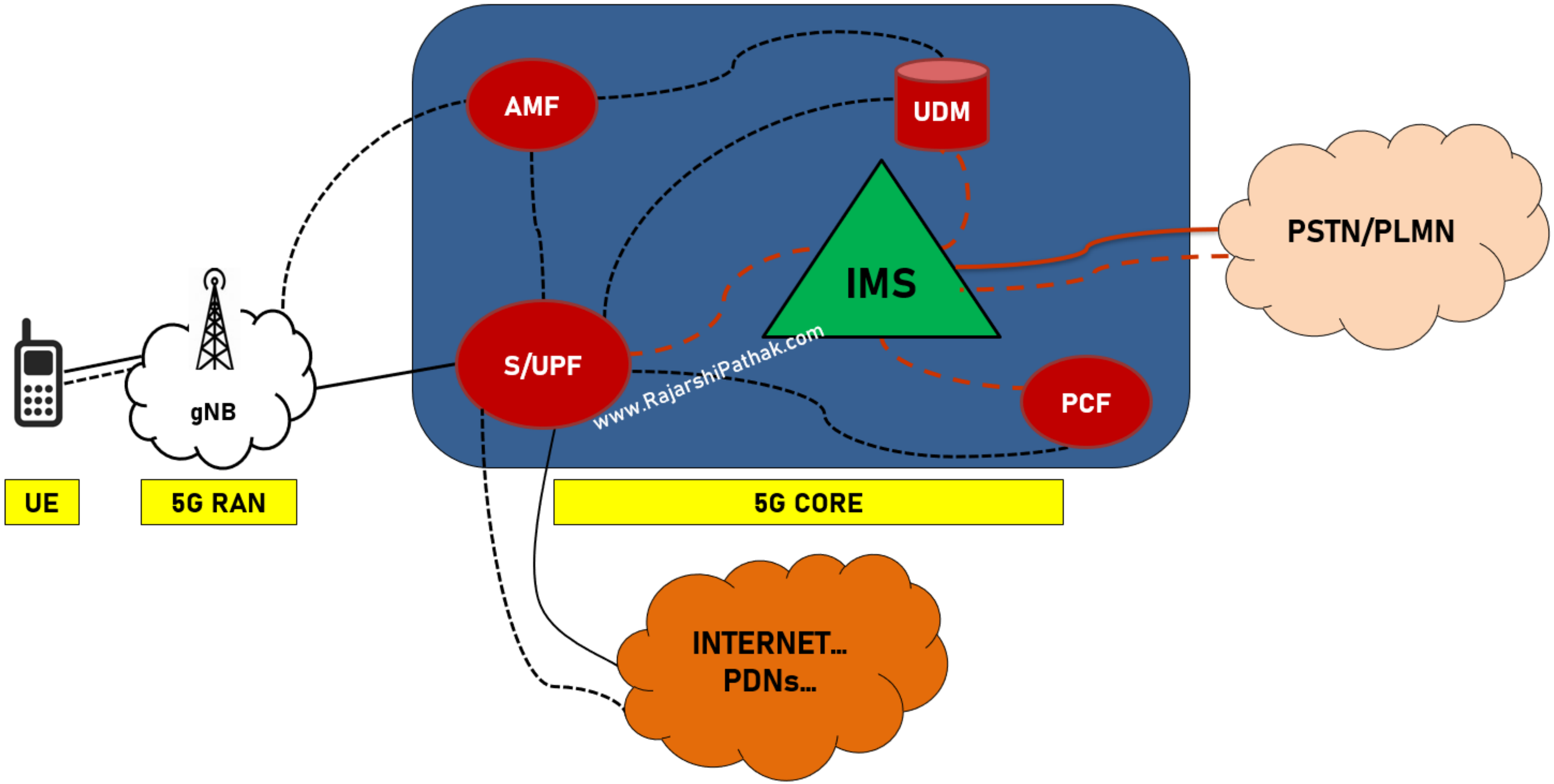


Important nodes in IMS

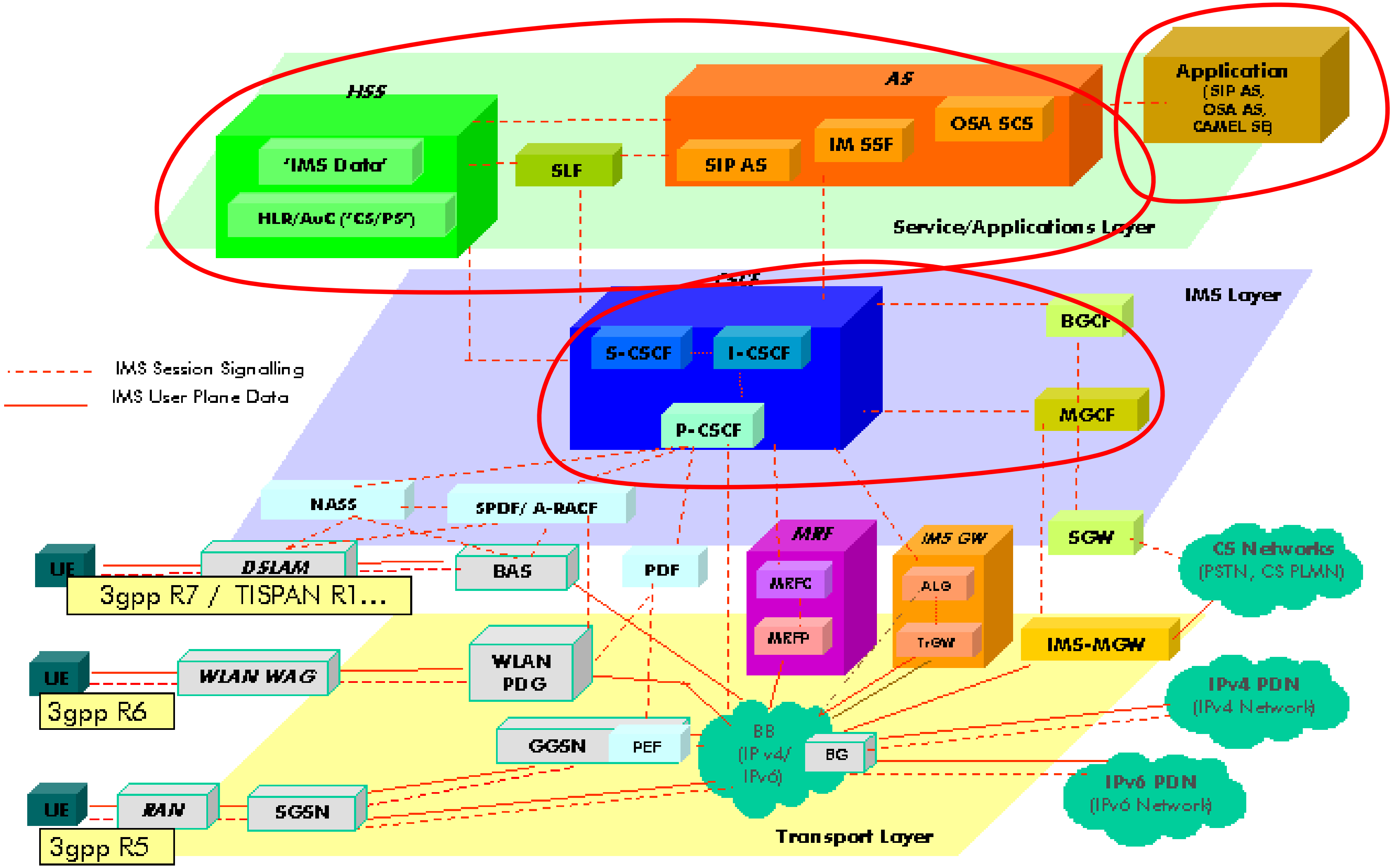
- CSCF - Call Session Control Function
- AF - Application Function
- MRF – Multimedia Resource Function
- MGCF – Media Gateway Control Function
- BGCF – Breakout Gateway Control Function
- IMS-GWF – Gateway Function
- HSS – Home Subscriber Server (4G)
  - Unified Data Management (5G)

- Nodes deployed over the cloud/datacenter as other 5G Core nodes

Where is IMS? (5G)



Where is IMS ? (4G)



S-CSCF

- Serving - CSCF
  - Controls the user’s SIP Session
  - very few per domain
  - Located in the home domain
  - Is a SIP registrar (and proxy)

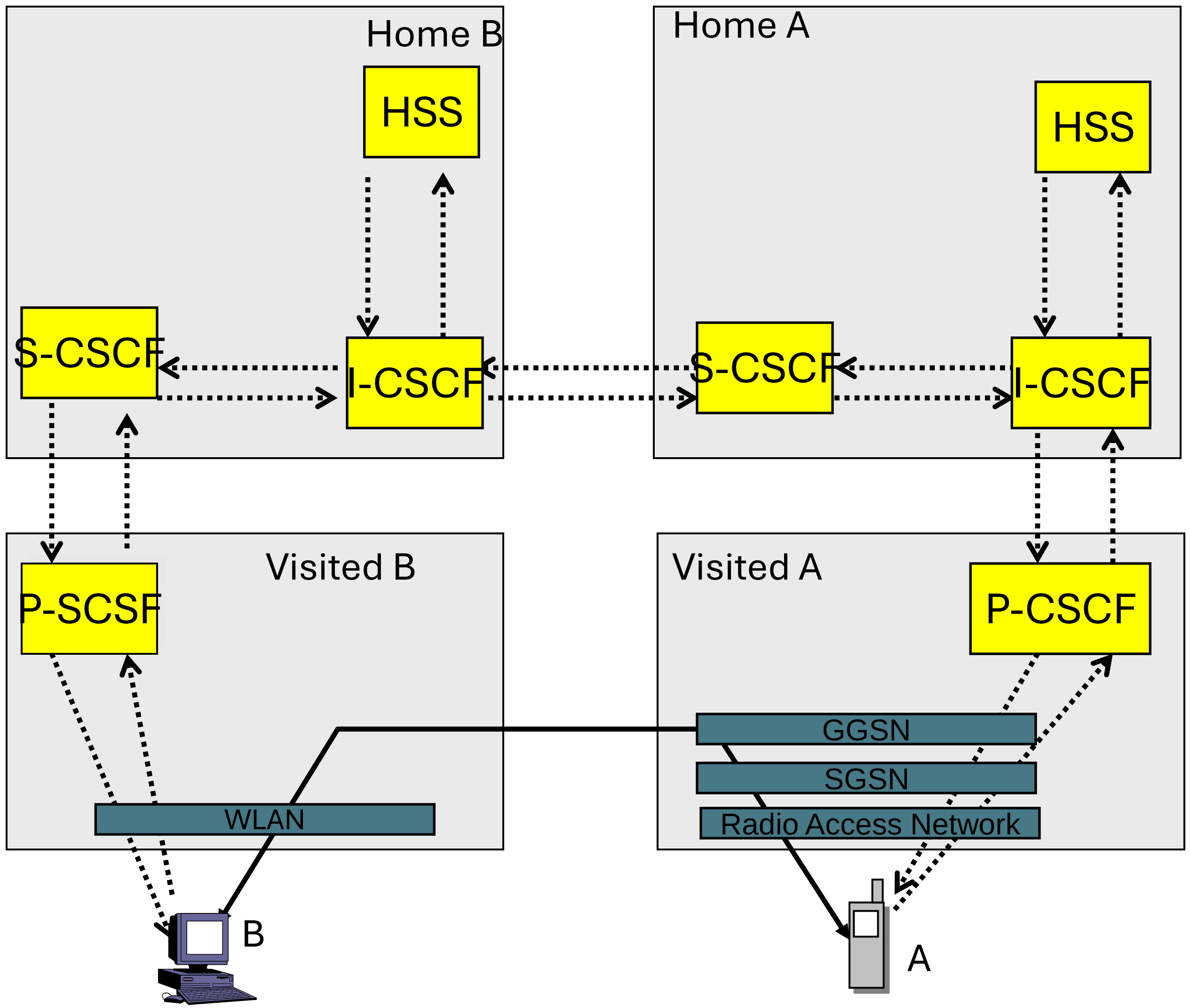
P-CSCF

- IMS contact point for the user’s SIP signaling
- Several in a domain
- Located in the visited domain
- Terminals must know this proxy (e.g. DHCP used)
- Compresses and decompresses SIP messages
- Secures SIP messages
- Assures correctness of SIP messages

I-CSCF

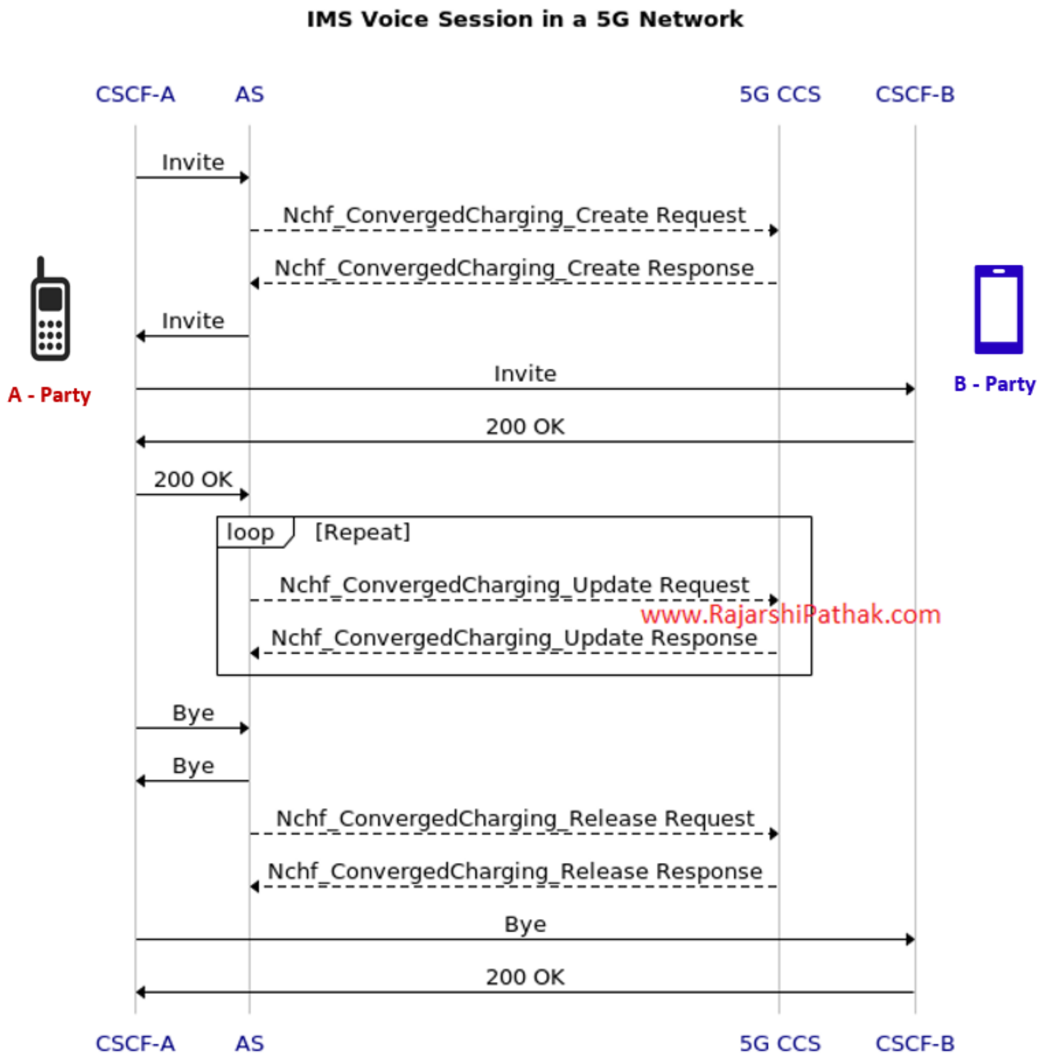
- domain’s contact point for inter-domain SIP signaling
- one or more per domain
- In case there are more than one S-CSCFs in the domain, locates which S-CSCF is serving a user

4G IMS: basic call flow



Non-GPRS
access
Networks
(e.g. WLAN)
comes in release 6

5G IMS: basic call flow



- IMS nodes communicate in SIP
- 5G Converged Charging System (CCS) communicates in HTTP/2 REST
- CSCF and AS perform authentication and service authorization
  - Checks for balance/credit
- The session gest established (Invite)
- Subsequent charging updates can be done via the CCS
- Session is finished via Byes

IMS→Non-IMS communications

- The IMS detects that the call destination is not a IMS user
- Triggers the BGCP to forward SIP signalling to the MGCF
- SIP messages are converted to ISUP (ISDN User Part)
  - Protocol to support voice and non-voice signalling in telefone comms.
- The converted messages are sent to the network (Public Land Mobile Network) via the MGW