Cisco Expo
2012

IP Mobility
Protocols and Architectures

Martin Kramolis, CCIE #4738

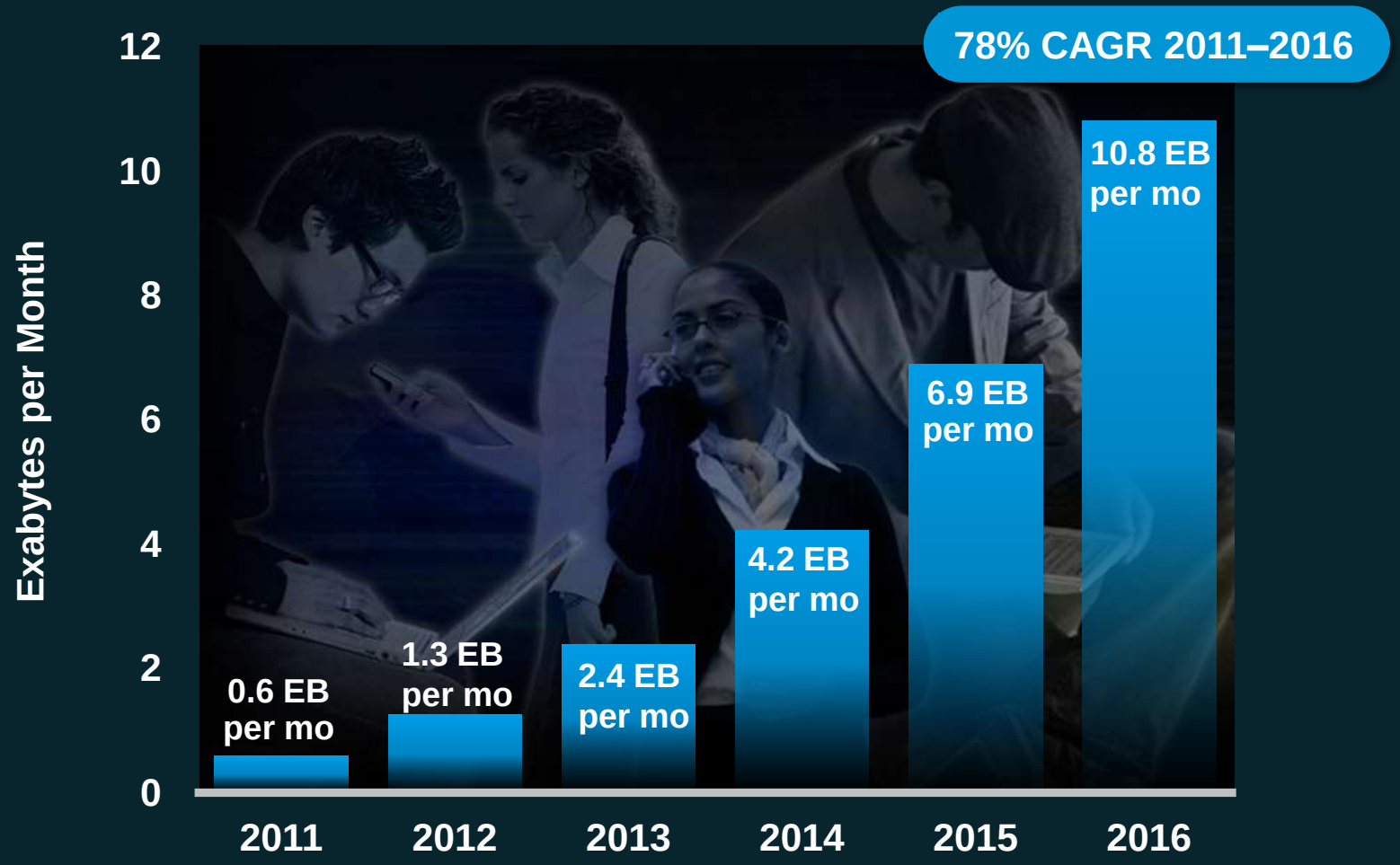
Agenda

- What is Session Persistency. Why Session Persistency?
- Session Persistency facts
- Applications and user expectation
- What is available for Session Persistency?
- Some Protocols and Architectures in detail
- Conclusion
- Q&A

Why Session Persistency

Global Mobile Data Traffic Growth / Top-Line

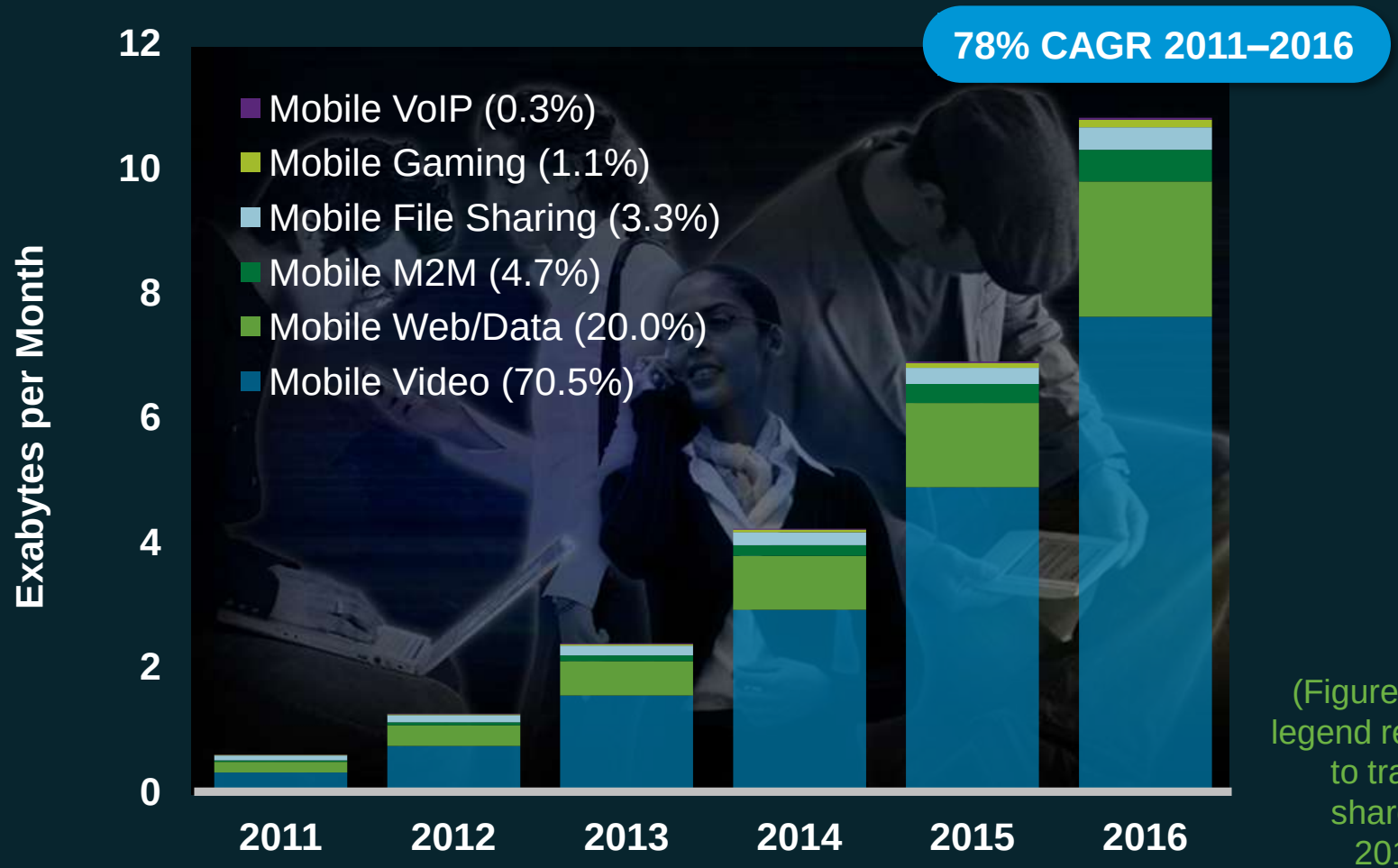
Global Mobile Data Traffic will Increase 18X from 2011 to 2016



Source: Cisco Visual Networking Index (VNI) Global Mobile Data Traffic Forecast, 2011–2016

Global Mobile Data Traffic Growth / Apps

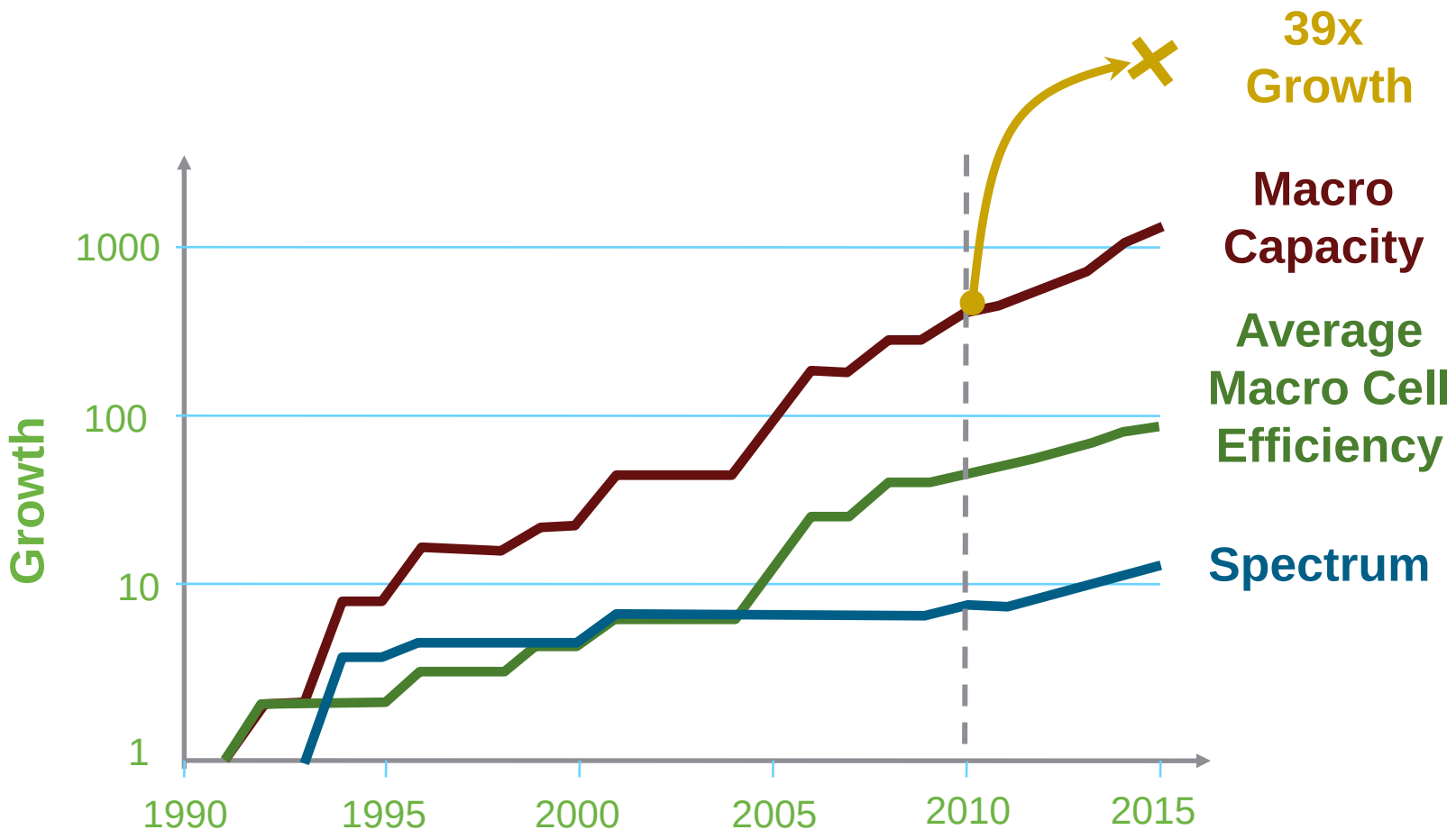
Video to Exceed 70 Percent of Mobile Data Traffic in 2016



(Figures in legend refer to traffic share in 2016.)

Source: Cisco Visual Networking Index (VNI) Global Mobile Data Traffic Forecast, 2011–2016

Scaling the Mobile Internet
Delivering 39 fold increase in Supply



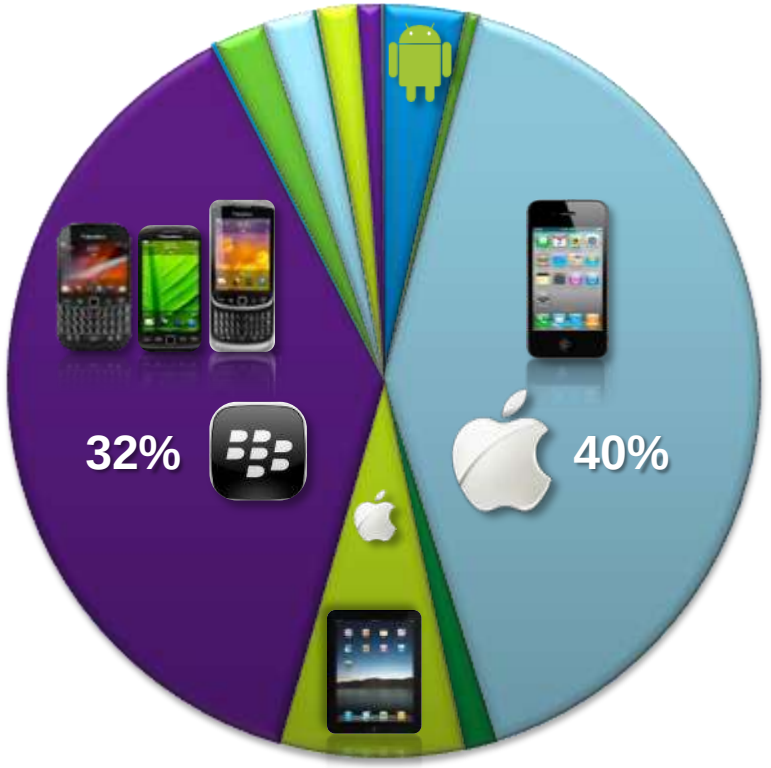
Source: Agilent

Media Rich Mobile Tablets and Devices

Devices—Everyone's Got One

Platform	July 2010	July 2011
iPhone	5,895	17,337
	22%	40%
iPad	677	5,933
	2%	14%
BlackBerry	14,910	13,917
	55%	32%
Android	209	3,822
	1%	9%
Others	5,433	2,049
	20%	5%
Total	**27,124**	**43,058**

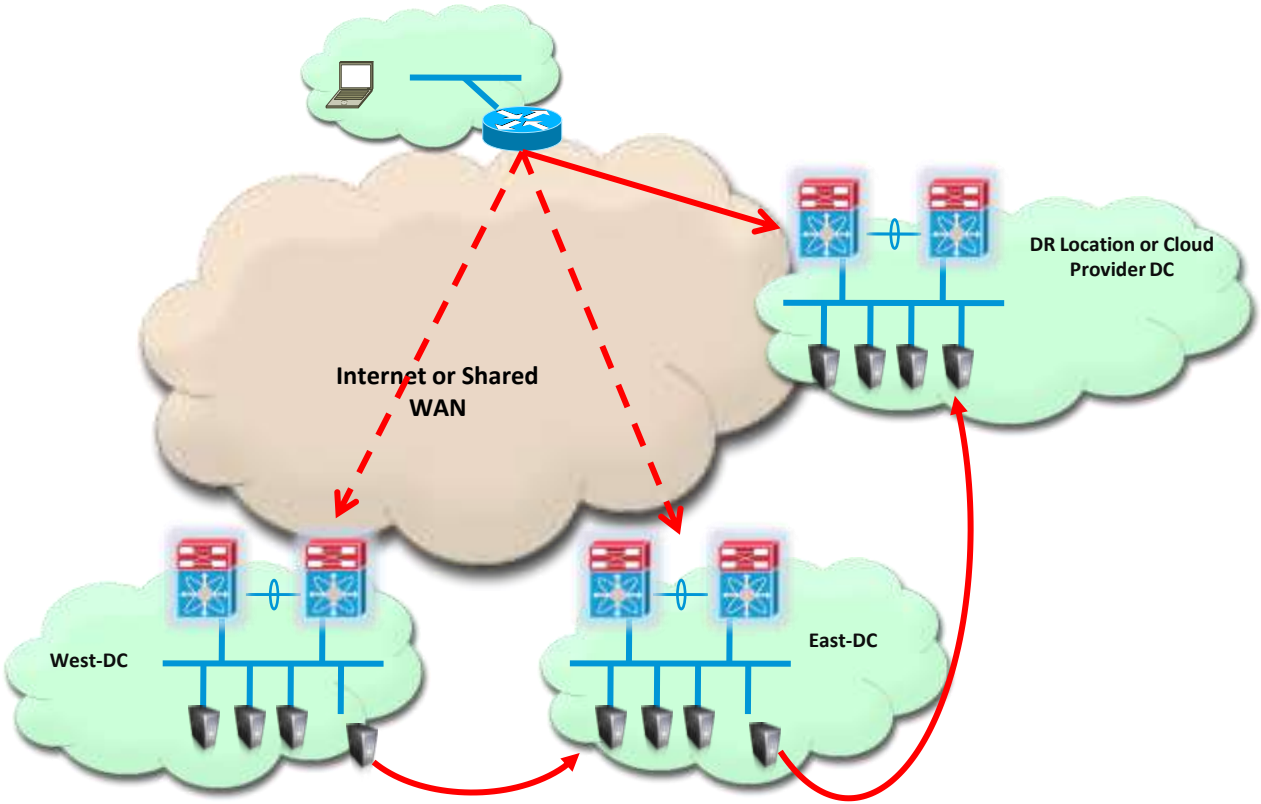
Smartphones and Tablets at Cisco, July 2011



Cisco's total mobile device count **grew 59% in 12 months**.

Virtual Machine Mobility

Session Persistency relevance to Data Centre



Session Persistency Relevance

- At home (~35%)
  - Mobile operator:: Nice add-on for WiFi offload, but not needed
  - User:: Not a really problem as I'm always within reach of my WiFi AP
- In the office (~25%)
  - Mobile operator:: Nice add-on for WiFi offload, but not needed
  - Enterprise:: Need for roaming between WiFi Access Points, VM Mobility.
- On the Go (~40%)
  - User:: I like it. This is what makes mobile Internet mobile.
  - Mobile operator:: I can extend my coverage. I can benefit also from WiFi offload.

Session Persistency Facts

User experience is what defines session persistency

- Quality of persistence is what is the key :
  - No perception of any change by user
  - Application stalls and resumes
  - Application stalls and can not recover
- Some applications may be more sensitive than others in the sense that the use experience is more degraded.
- Main question : what is a session ?
  - An IP transport/session flow identified by some ID
  - An application flow identified by some application ID (HTTP cookie, Video ID, Application state maintained on both sides)
  - Other …

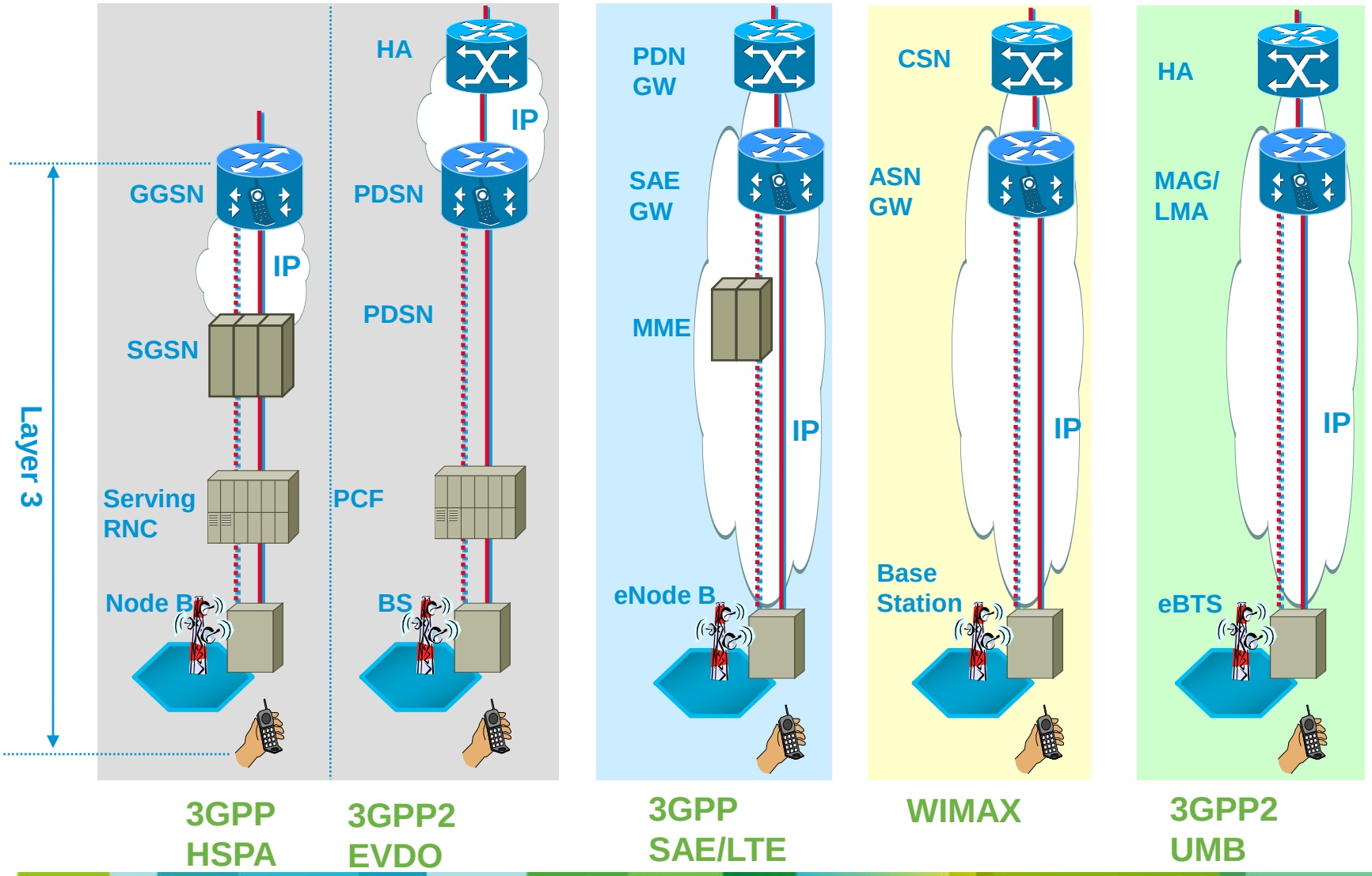
User experience is what defines session persistency

Differtent applications, different user experience

- **Web browsing**
- **Email**
- **IM**
- **VPN**
  - **AnyConnect**
- **Video Streaming**
  - **Netflix**
  - **SlingBox**
  - **VOD**
  - **Youtube**
- **Business & productivity tools**
  - **SAP**
  - **Business Object**
- **Real Time Conferencing**
  - **Voice (looking at VOIP)**
  - **Video**
  - **WebEx**
  - **Skype**
  - **Fring**

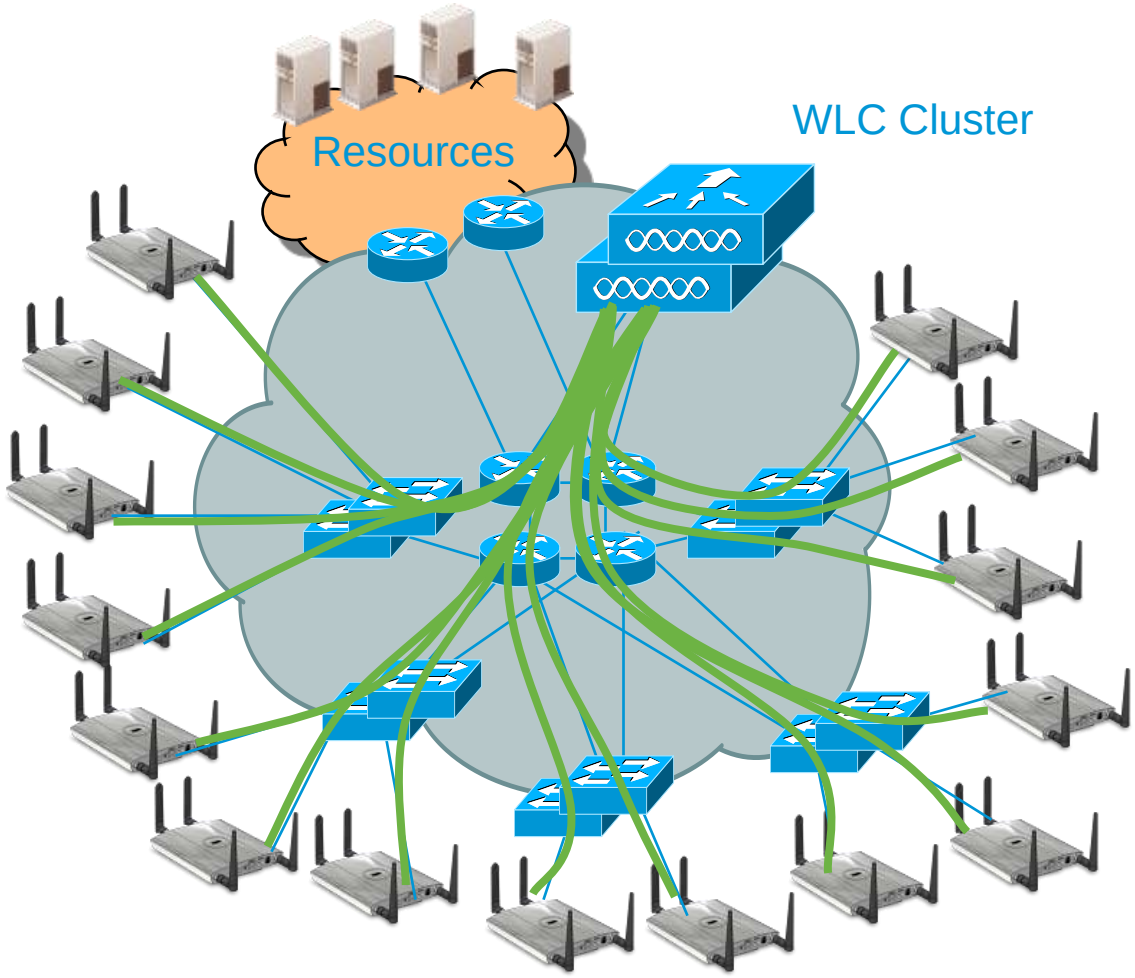
Network Anchor in the Cellular Architectures

Cellular Architectures are Converging



Network Anchor in the 802.11 environment

- LWAPP/CAPWAP Infrastructure bring an anchor point for the 802.11 networks

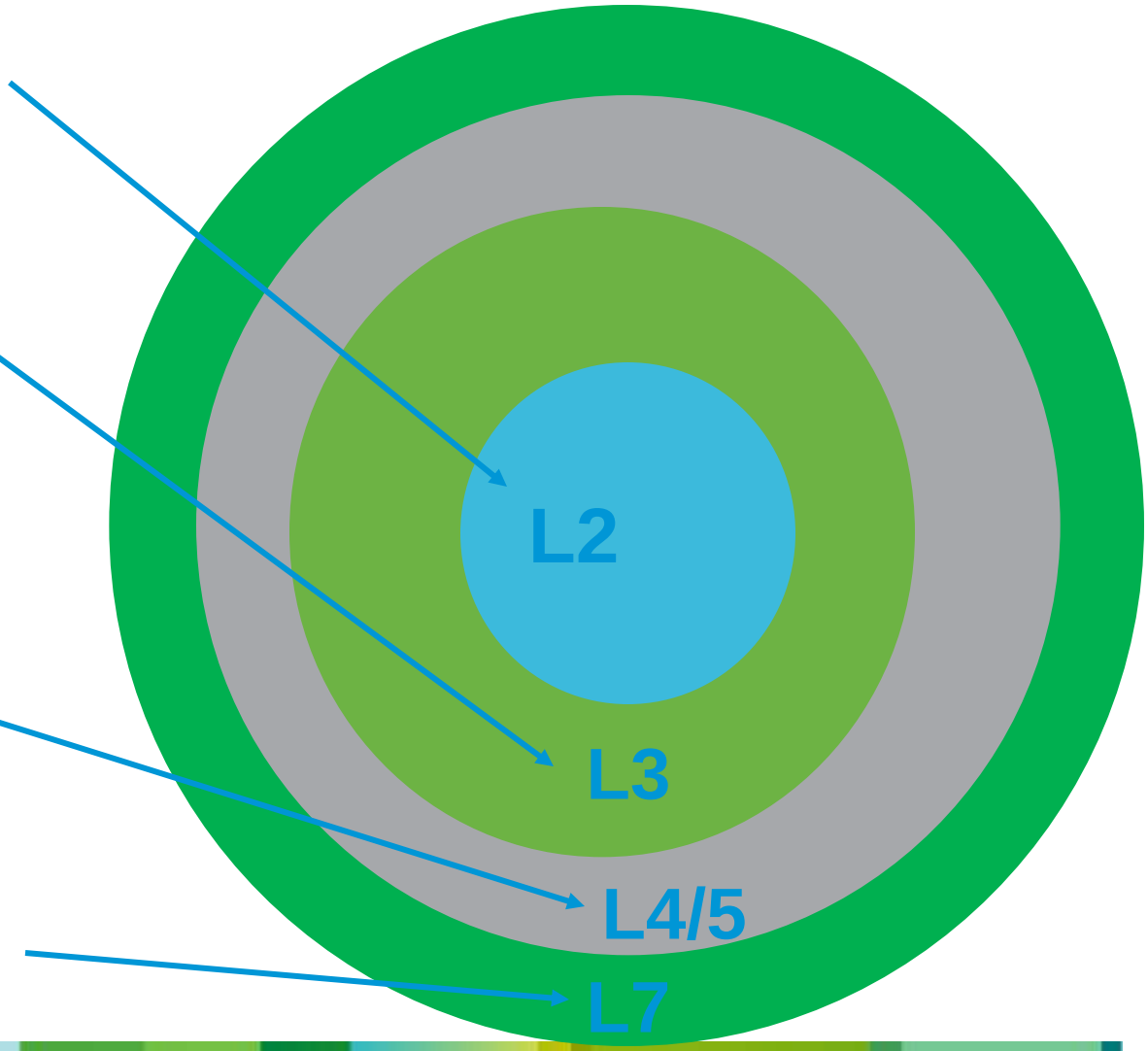


Mobility / Session Persistence Mechanisms

- **Layer 2 solutions : the link layer remains unchanged**
  - Ethernet STP
  - Ethernet over IP encap / CAPWAPP
  - PPP / GTP
- **Layer 3 solutions : the « IP address » remains unchanged**
  - Host routing / Cisco LAM : only scales in a limited domain
  - MIPv4/v6, DSMIP, PMIP
  - MobIKE
  - Any VPN solution with auto-reconnect
  - LISP
  - HIP
- **Layer 4 solutions : the transport layer allows layer 3 changes & multihoming**
  - SCTP multihoming
  - Multipath TCP
  - ILNP
- **Application-Layer solutions : persistency is handled at application layer**
  - SIP mechanisms using SIP Re-Invites
  - TCP Migrate
  - SSL reconnect (WebEx)
  - Application reconnect (L7 Mobility)
  - Adaptive Video

Mobility & the OSI Layers

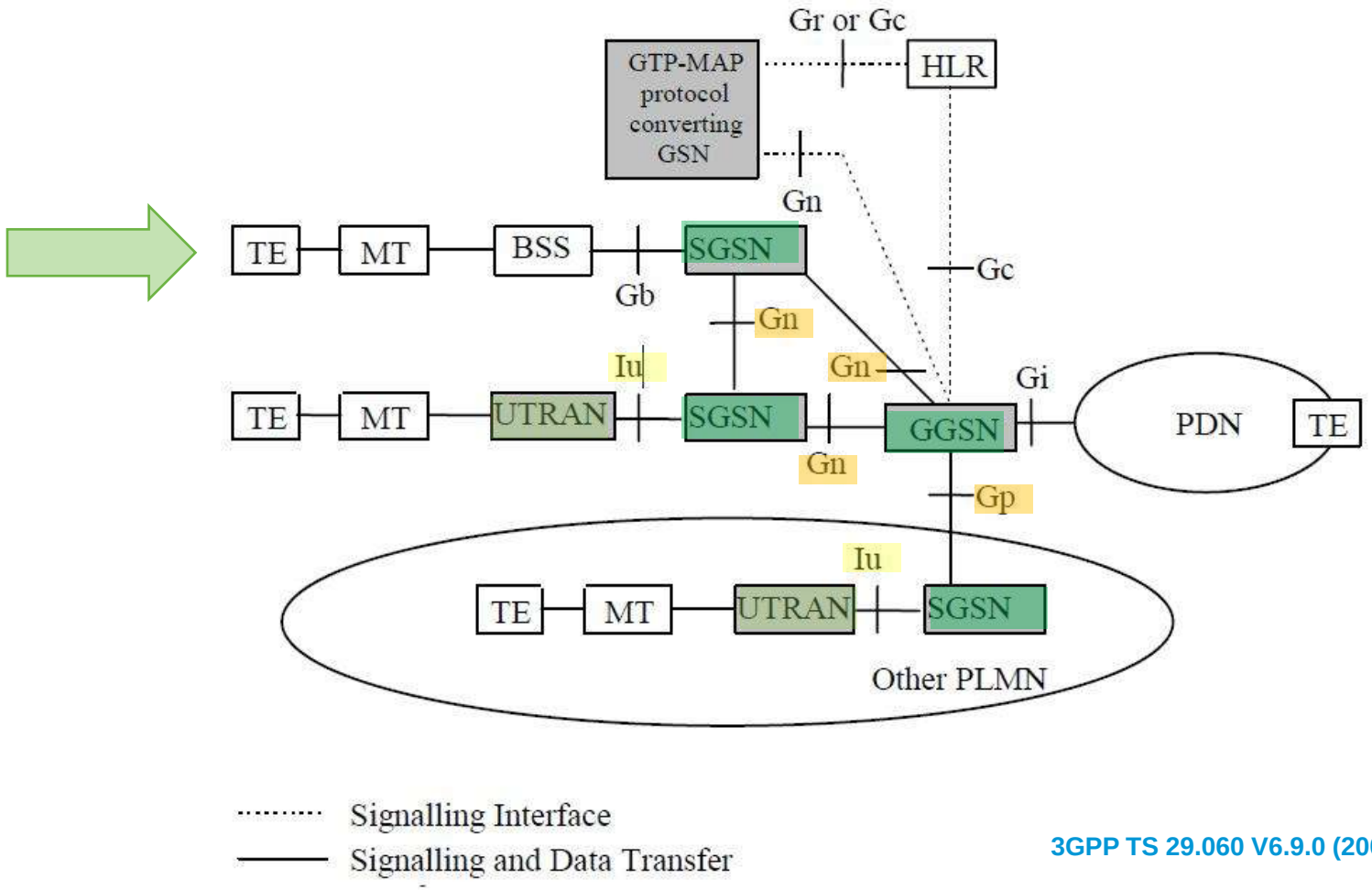
- L2 is fast, but not scalable
- L3 scales well, support multiple L2 links and is application independent
- L4/5 session management provides end to end session identification, path optimization
- Application layers provide application recovery when all else has failed. Can be very application specific



Some Protocols in Detail

GTP

GPRS System Logical Architecture

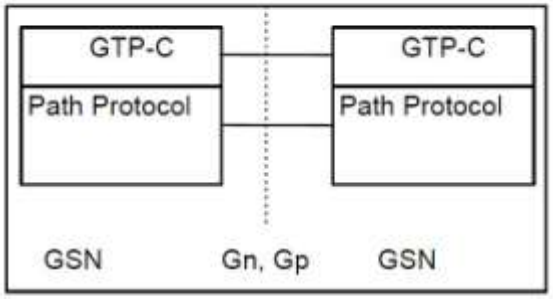


3GPP TS 29.060 V6.9.0 (2005-06)

GTP-C/GTP-U Planes

GTP-C: Control Plane signaling facilitates *Creation, Modification* and *Deletion* of GTP tunnels.

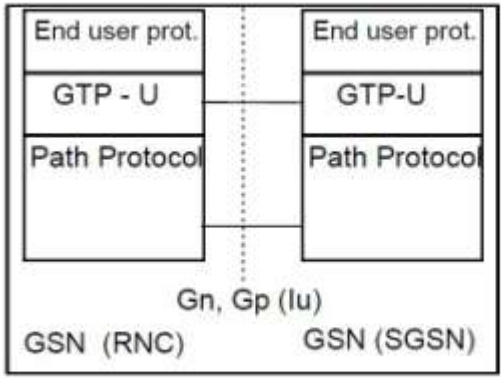
- **Path Protocol UDP port, registered port *2123***



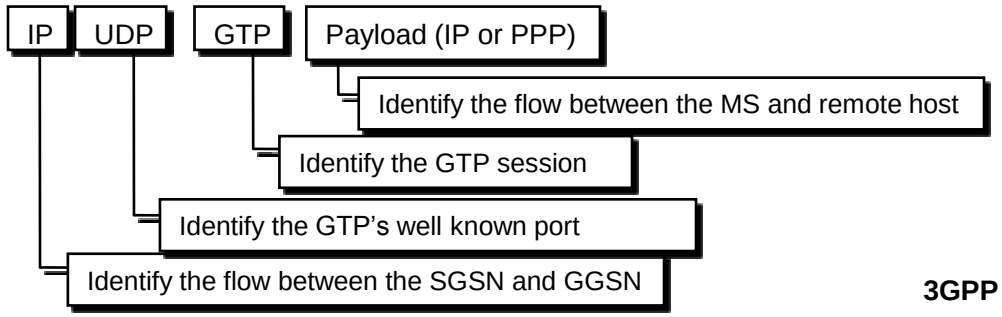
Signalling Plane - Protocol Stack

GTP-U: User Plane tunneling mechanism to service user *data traffic* transmission

- **Path Protocol UDP, registered port: *2152***



GTP-U - Protocol Stack (GTP-U over the Iu in brackets)

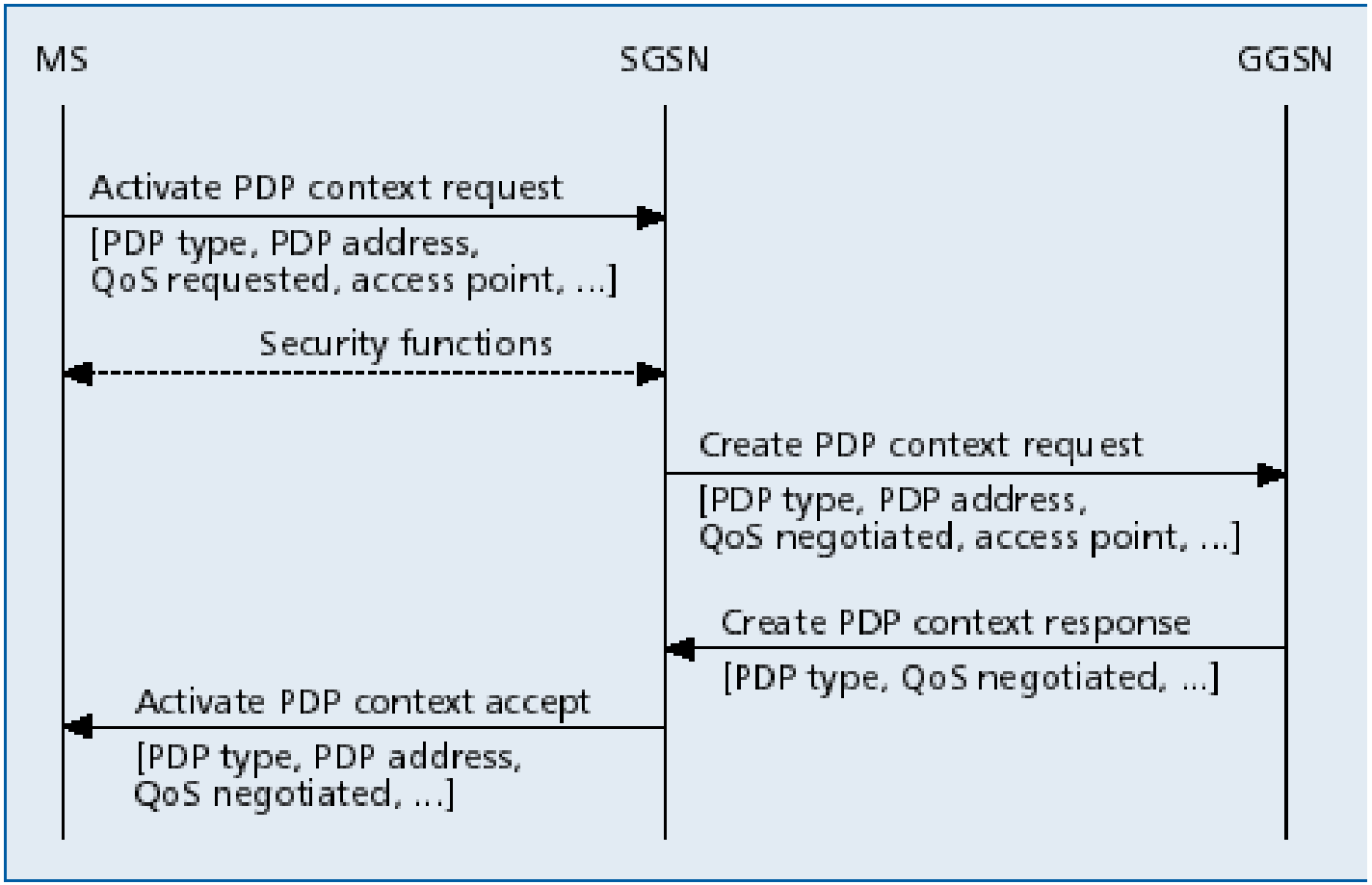


3GPP TS 29.060 V6.9.0 (2005-06)

GTP Message Types

1	Echo Request (GTP-C, GTP-U, GTP') – Path management
2	Echo Response (GTP-C, GTP-U, GTP') – Path management
3	Version Not Supported (GTP-C) – Path management
4	Node Alive Request (GTP')
5	Node Alive Response (GTP')
6	Redirection Request (GTP')
7	Redirection Response (GTP')
8-15	For future use. Shall not be sent. If received, shall be treated as an Unknown message.
16	Create PDP Context Request (GTP-C) – Tunnel mgmt.
17	Create PDP Context Response (GTP-C) - Tunnel mgmt
18	Update PDP Context Request (GTP-C) - Tunnel mgmt
19	Update PDP Context Response (GTP-C) - Tunnel mgmt
20	Delete PDP Context Request (GTP-C) - Tunnel mgmt
21	Delete PDP Context Response (GTP-C) - Tunnel mgmt

PDP Context activation procedure



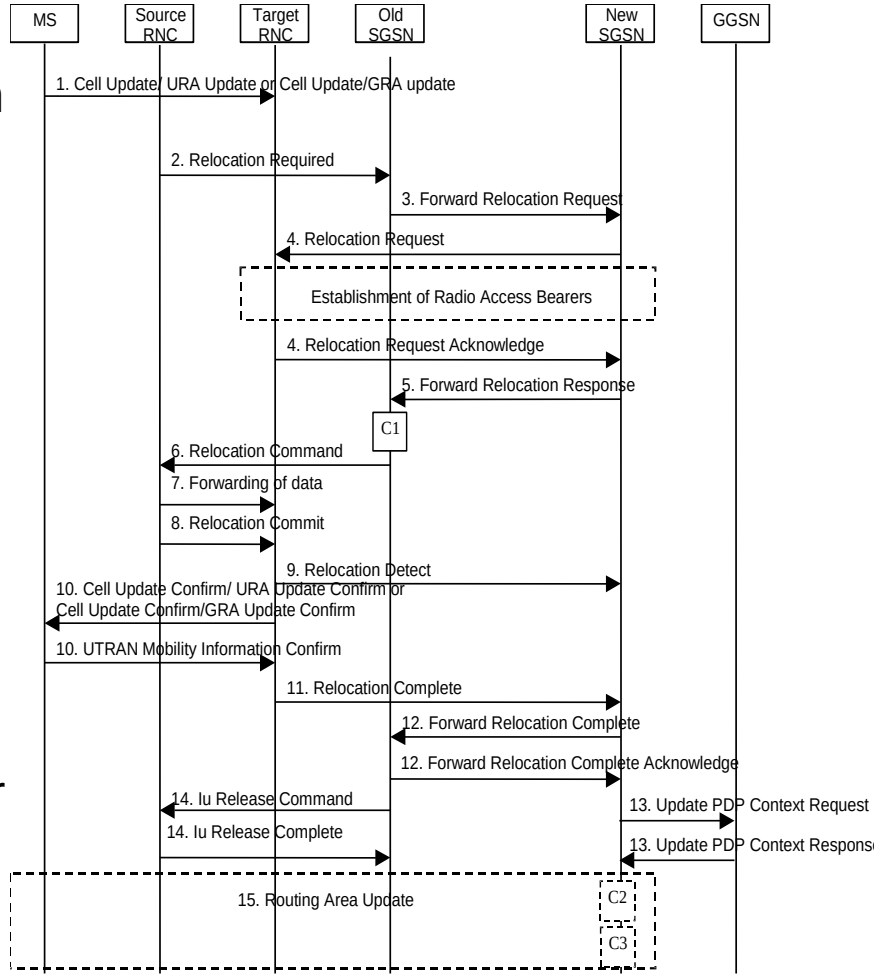
Mobility Example

3GPP TS 23.060 6.9.2.2.3

1) When MN moves to new SGSN, context transfer happens between old and new SGSNs

2) New SGSN sends GTP-C message to GGSN, identifies IMSI that arrived and provides GTP-U tunnel endpoint and session identifier(s), as well as QoS profile

3) GGSN sends GTP-C message for acknowledgement

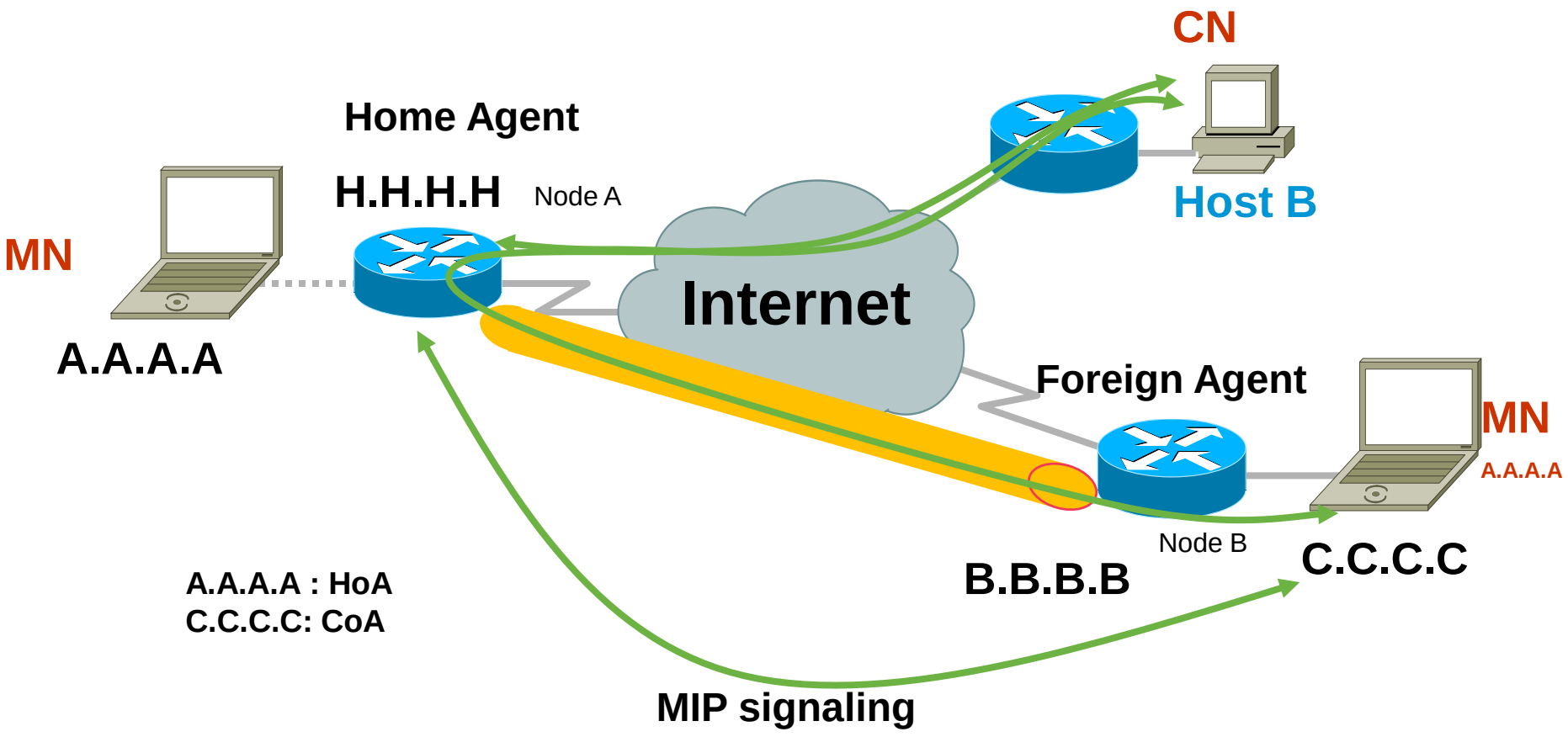


GTP Summary

- Protocol includes mobility management function
- Identifiers for subscriber (IMSI), phone number (MSISDN), IP Address, Access Point Name, PDP context (NSAPI)
- Independent Tunnel Endpoints for Control and Data Plane
- QoS Profile
- Optional user authentication
- No authentication for GTP messages in trusted GPRS network

MIP/PMIP/DSMIP

Mobile IP Concepts



Mobile IP Overview

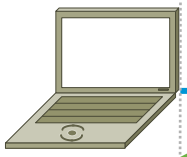
- Mobile IP concepts
- Mobile IPv4
- Mobile IPv6
- Dual Stack Mobile IPv6
- Proxy Mobile IPv6

What is Mobile IP ?

> **“Mobile IP provides an IP node the ability to retain the same IP address and maintain uninterrupted network and application connectivity while traveling across networks ”**

An “always on” IP service availability independent of location, movement, or infrastructure

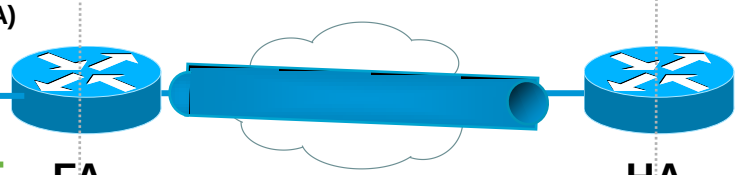
Mobile IP in a nutshell



MN
1.1.1.7

Solicitation (224.0.0.2)

MN optionally might solicit for an Agent (FA or HA)
Solicitation prompts FA or HA to send an advertisement



FA **HA**

Advertisement (224.0.0.1)

FA/HA advertise their presence via IRDP
MN detects movement by network prefix
MN obtains CoA from advertisement

Registration Request Sequence (UDP port 434)

MN sends unicast registration request to FA (UDP Destination Port=434)
Request includes Type of "MN's Address, HA, CoA, authenticator, Tunnel type, Lifetime, Broadcast…"
FA inspects the request. If no objections, FA "relays" the request to the defined HA

Registration Reply Sequence (UDP port 434)

HA
Inspects the request (can it fulfill options requested, performs authorization check)
If okay, HA adds a Mobility Binding that associates the MN home IP Address with the CoA
HA then builds a Layer 3 tunnel to the CoA (FA or direct to MN), if one doesn't already exist
Sends Registration Reply (UDP DestPort=UDP SrcPort from request) to the CoA (FA or direct to MN)

FA
Inspects the reply, if no objections "relays" the reply to the MN
Adds MN to list of visitors
Acts as default router for MN packets

HA
Sends out a Gratuitous ARP associating MN Home IP address with the HA's MAC address
Responds to ARP requests for MN Home IP address with HA's MAC address
Keeps an eye out for packets routed to the MN's IP address and redirects them to the current CoA

MN
If authorized, MN is now set to maintain active or future application traffic
If rejected the MN can inspect the return code and attempt to re-register

De-registration Request (UDP port 434)

MN
Detects it's on home subnet
Sends Registration Request with a lifetime of 0

Tunnel mode

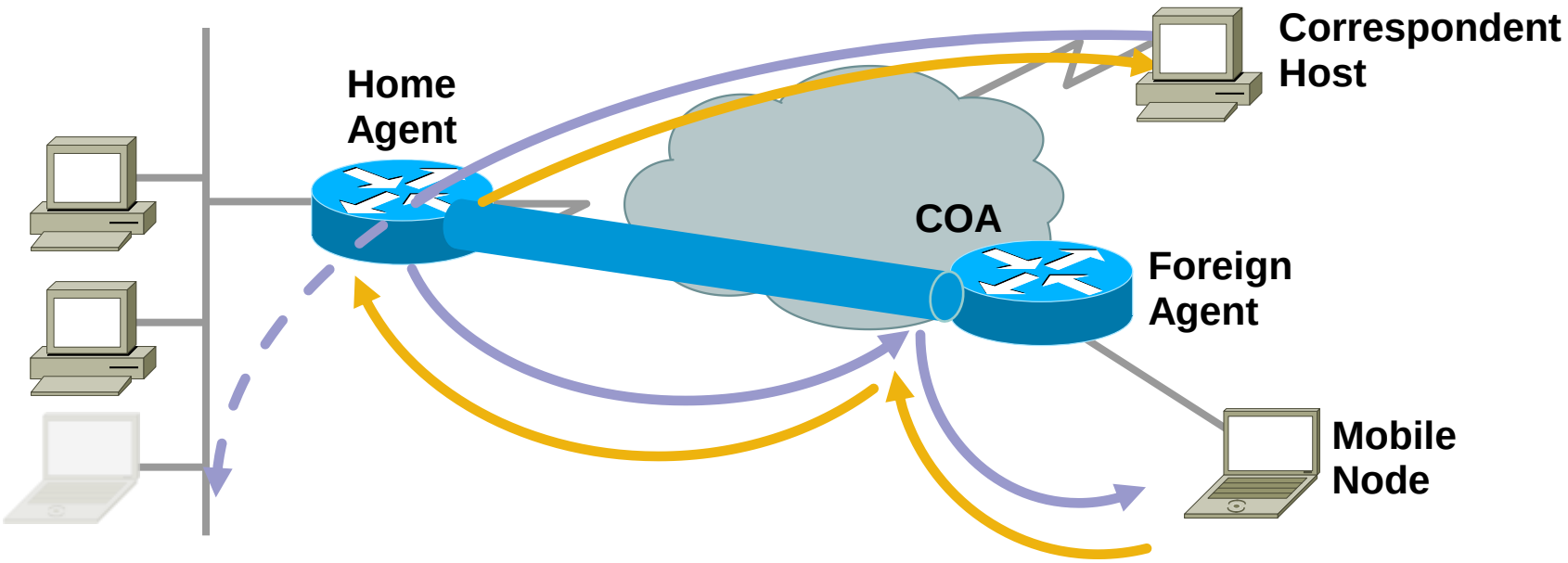
- CoA mode :

  FA shares same IP address with multiple MN's. Tunnel terminates at FA. During early days, because of IPv4 address scarcity and not so powerful MN (FA de-tunnels pkts, less processing requirement at MN), bandwidth limitation on air (less traffic on air between FA and MN)

- CCoA mode :

  Each MN has different IP address. Tunnel terminates between MN and HA. No need of FA.

Reverse Tunneling



- Traffic is sent from the MN to the HA via the tunnel, then delivered via routing
- Solves the problem when packets from MN to CN get dropped due to ingress filtering, which, if enabled on a router, will cause the router to drop packets that have topologically incorrect source address

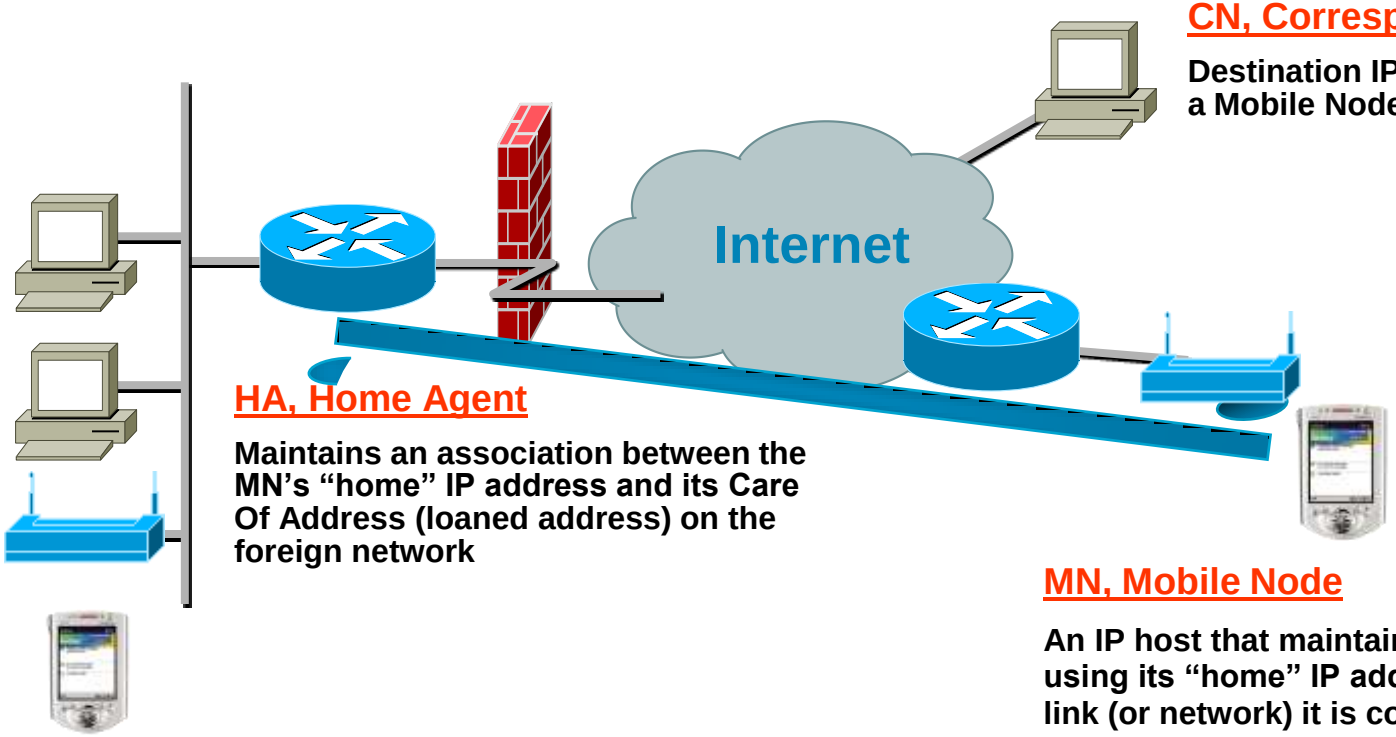
Mobile IP Overview

- Mobile IP concepts
- Mobile IPv4
- Mobile IPv6
- Dual Stack Mobile IPv6
- Proxy Mobile IPv6

Mobile IPv6 Protocol

- RFC 3775
- Similar to the Mobile IPv4 concept
  - A home agent keeps track of the mobile node's location
  - Including location discovery, movement detection, registration, and topology establishment
- Different from the Mobile IPv4
  - No Foreign Agent
  - Traffic can be sent directly between two communicating nodes

Mobile IPv6 – Key components



CN, Correspondent Node

Destination IP host in session with a Mobile Node

HA, Home Agent

Maintains an association between the MN's "home" IP address and its Care Of Address (loaned address) on the foreign network

MN, Mobile Node

An IP host that maintains network connectivity using its "home" IP address, regardless of which link (or network) it is connected to

MN

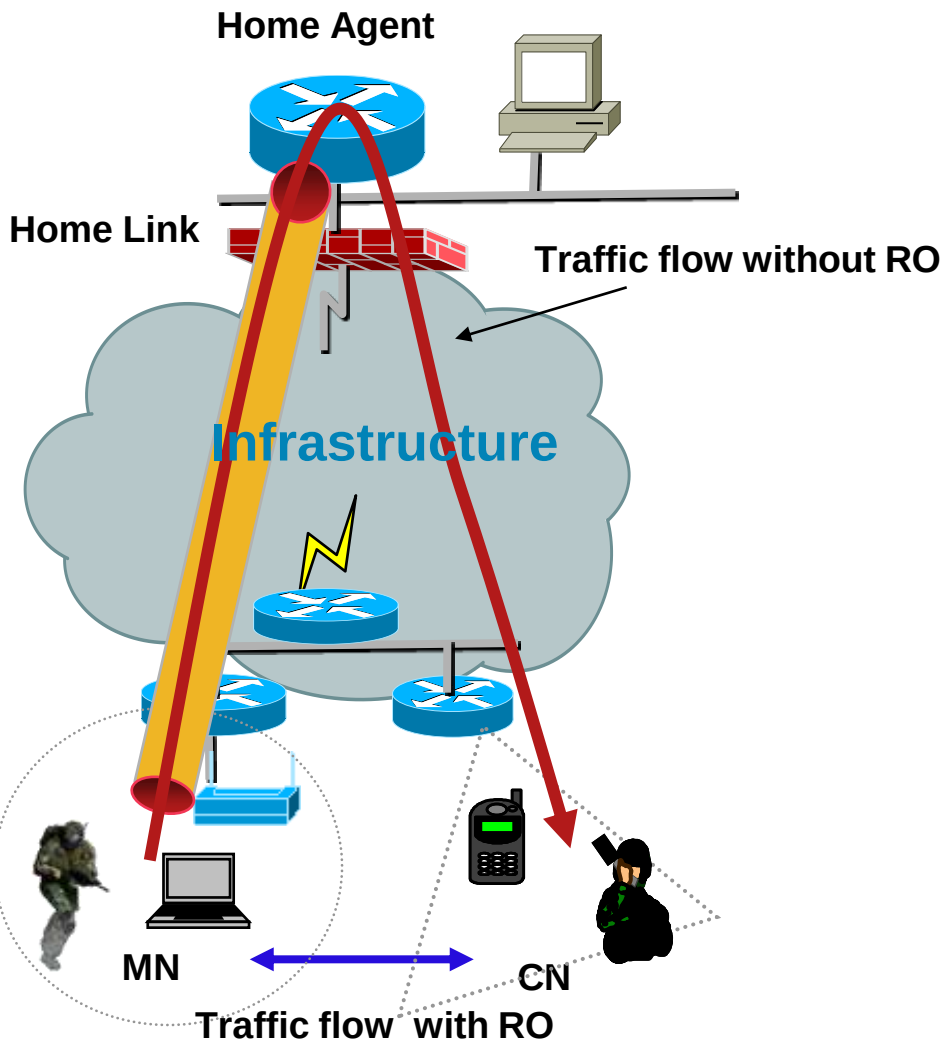
Mobile IPv6 Operations Overview

- MN acquires a new IPv6 address on visited networks (typically using auto-configuration) as its Care-of-Address (CoA)
- MN obtains its home address (HoA) and home agent address statically or acquires them dynamically
- MN informs its home agent (HA) about its CoA
- The HA intercepts traffic and tunnels to the MN
- MN can inform correspondent node (CN) about its CoA. CN and MN can communicate directly, bypassing the HA

Movement detected

Route Optimization (RO) in Mobile IPv6 Node

- Allows communication traffic to be sent directly without going through a home agent
- Advantages with RO
  - Reduce link bandwidth consumption
  - Decrease round trip time
  - Avoid a potential point of failure
- Disadvantages with RO
  - CN needs to be Mobile IP aware
  - Loose policy control



Mobile IP Overview

- Mobile IP concepts
- Mobile IPv4
- Mobile IPv6
- Dual Stack Mobile IPv6
- Proxy Mobile IPv6

Dual Stack Mobile IP (DSMIPv6)

- RFC 5555
- Extension of Mobile IPv6 to support IPv4 care-of address to carry IPv4 traffic via bi-directional tunnels between mobile nodes and their home agents.
- DSMIPv5 allows mobile nodes to manage mobility while moving within both IPv4 and IPv6 Internet
- When in IPv4 network, MN gets IPv4 CoA and registers it on HA.
- Both IPv4 and IPv6 home addresses are bound to the address.
- IPv4 traffic goes through IPv4-in-IPv4 tunnel between MN and HA.
- IPv6 traffic goes through IPv6-in-IPv4 tunnel between MN and HA.
- Similar as above when MN uses IPv6 CoA.

Mobile IP Overview

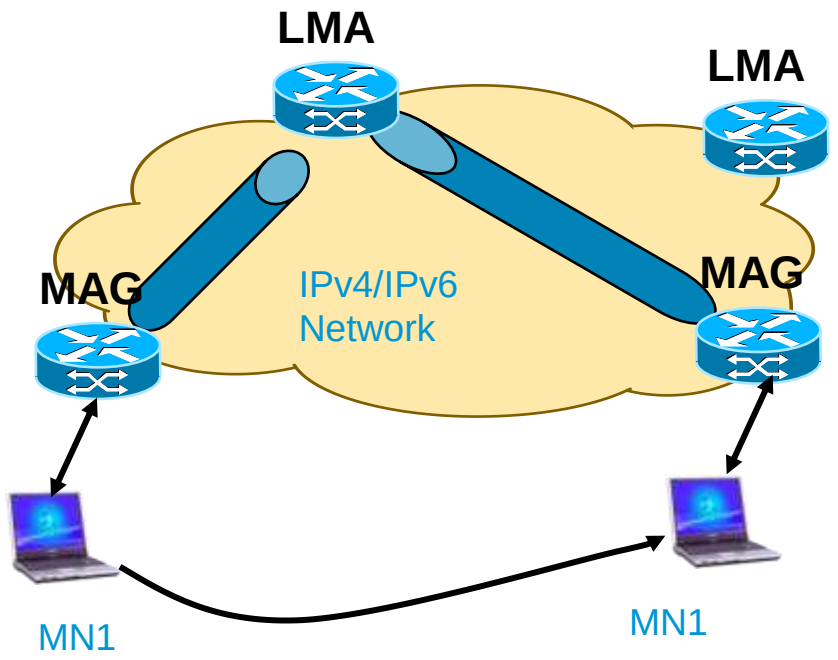
- Mobile IP concepts
- Mobile IPv4
- Mobile IPv6
- Dual Stack Mobile IPv6
- Proxy Mobile IPv6

WHAT is Proxy Mobile IPv6?

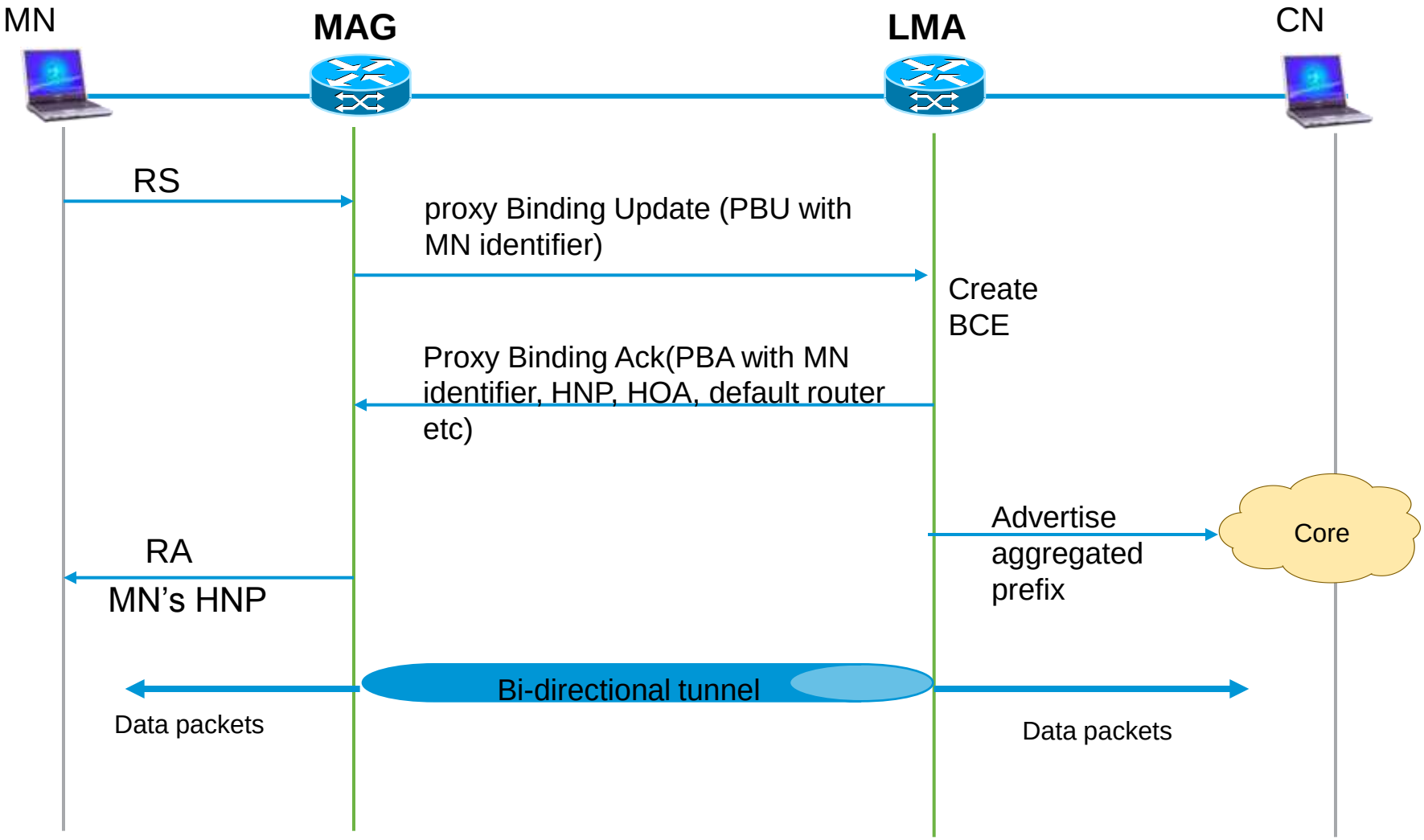
- This is network based mobility solution
- Mobile node is not aware when it moves to a new access “link”/ access router (i.e. home network emulation)
- Re-use of Mobile IPv6 protocol, though signaling and tunneling between access router and anchor router
- Enhancements for signaling between access router and anchor router to support many mobile nodes
- Enhancements for signaling for access routers to support mobile node moving between them (e.g. message sequencing)

Proxy Mobility Domain

- Mobility Entities:
  - –LMA: local mobility anchor
  - –MAG: Mobile Access gateway
- MN Addressing
  - –IPv4 or IPv6
  - –No CoA on MN like in MIP
- Tunneling mode
  - –IPV4/IPV6 over IPV6
  - –IPV4/IPv6 over GRE-IPV4/IPv6
  - –IPV4/IPV6 over IPv4



PMIP signaling call flow



SCTP

SCTP

- RFC 4960 : Stream Control Transmission Protocol
- RFC 5061 : Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration

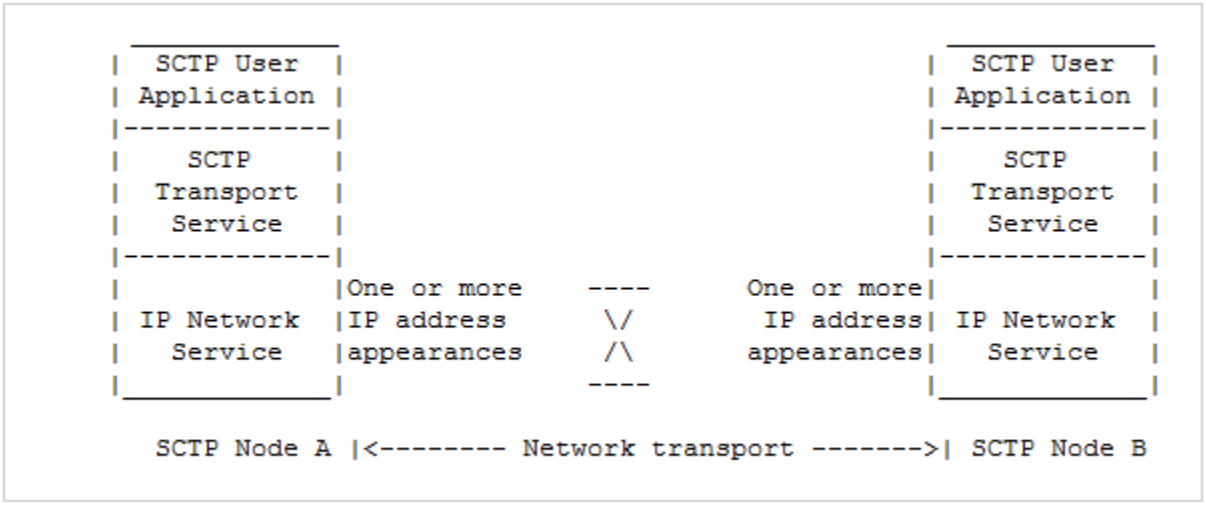
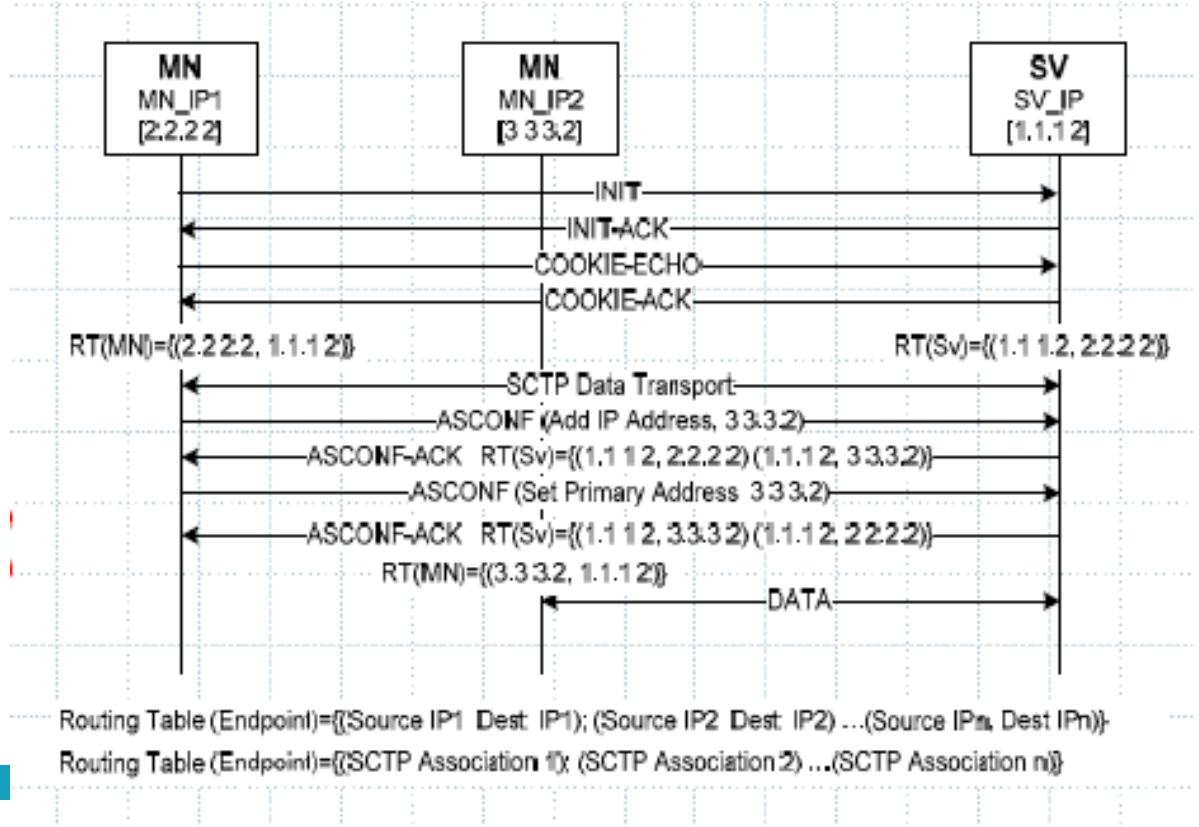


Diagram showing the concept of an SCTP association

SCTP Call Flow

- The association establishment in SCTP, uses the four-way handshake.
- During association startup, a list of transport addresses (i.e. IP address-port -pairs) is provided between the communicating entities.
- The ADDIP extension used in mSCTP supports dynamic address reconfiguration.



Summary

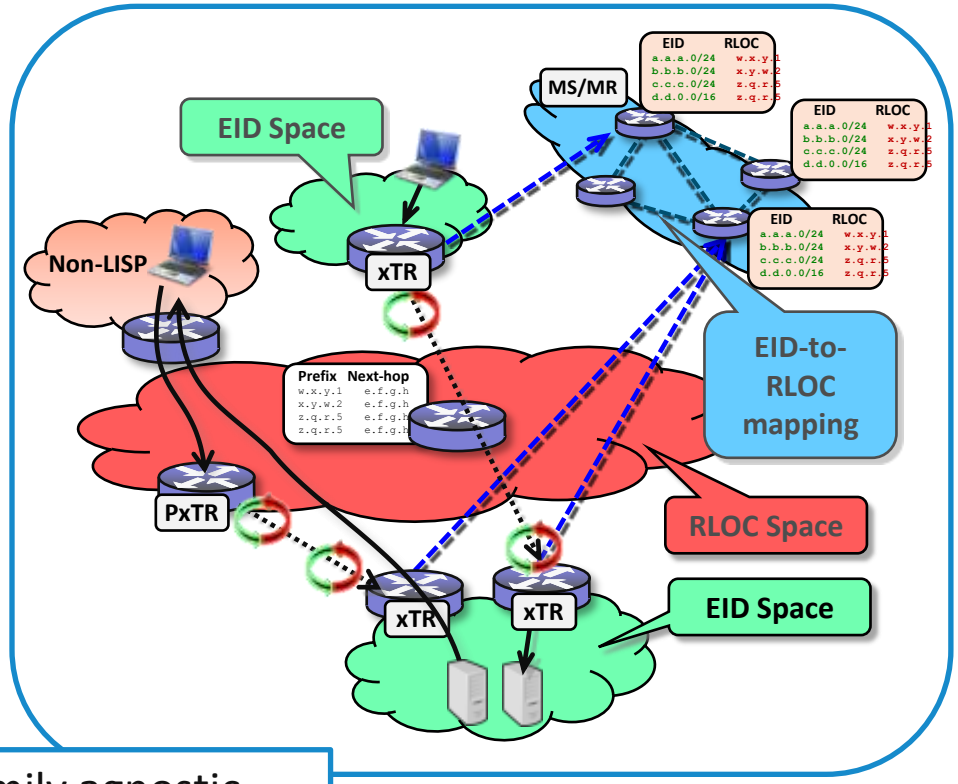
- SCTP has many tempting performance characteristics regardless of whether it is used for mobility. It's worth enabling.
- SCTP can run over any underlying mobility mechanism.
- Can be used in many scenarios with backward compatibility for evolution from TCP/UDP.
- Since you have SCTP anyway, the thought of using it for mobility arises naturally.
- The more knowledge that is exposed to SCTP, the better it does with both transport performance and mobility.
- Evolutionary migration is possible.

LISP

LISP - A level of indirection for IP addressing

Main attributes of LISP

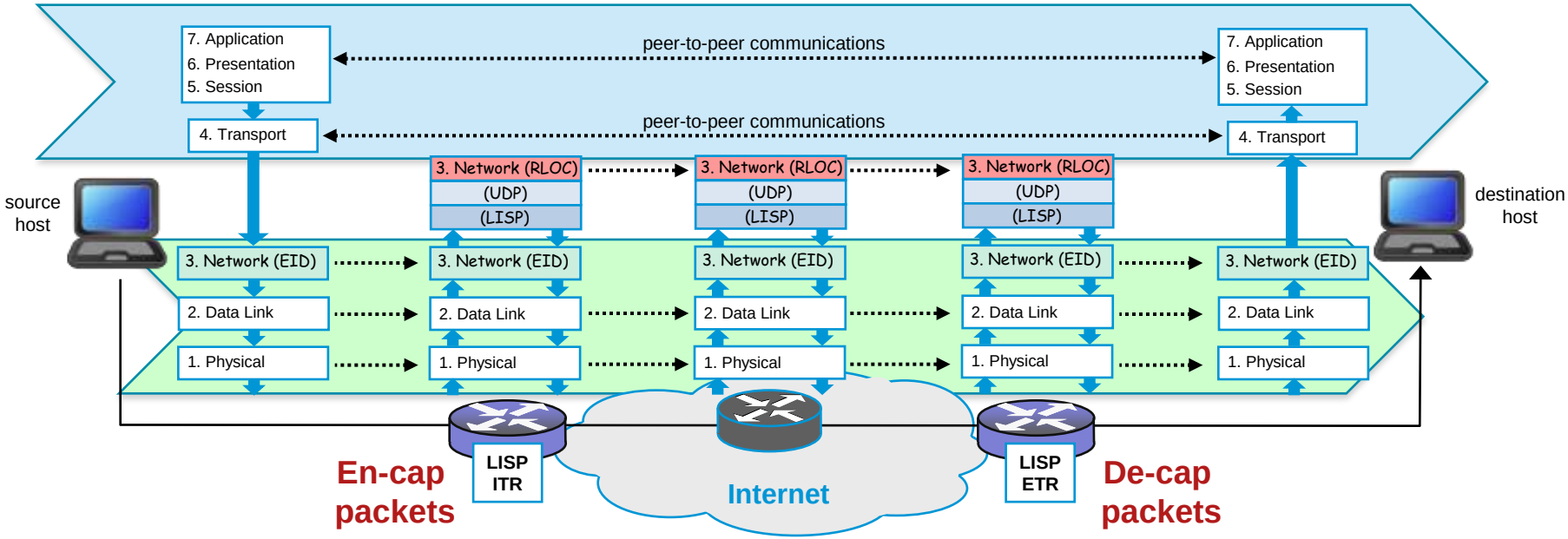
- **EID (Endpoint Identifier)** is the IP address of a host – just as it is today
- **RLOC (Routing Locator)** is the IP address of the LISP router for the host
- **EID-to-RLOC mapping** is the distributed architecture that maps **EIDs** to **RLOCs**



- Network-based solution
- No host changes
- Minimal configuration
- No DNS changes
- Address Family agnostic
- Incrementally deployable (support LISP and non-LISP)
- Support for mobility

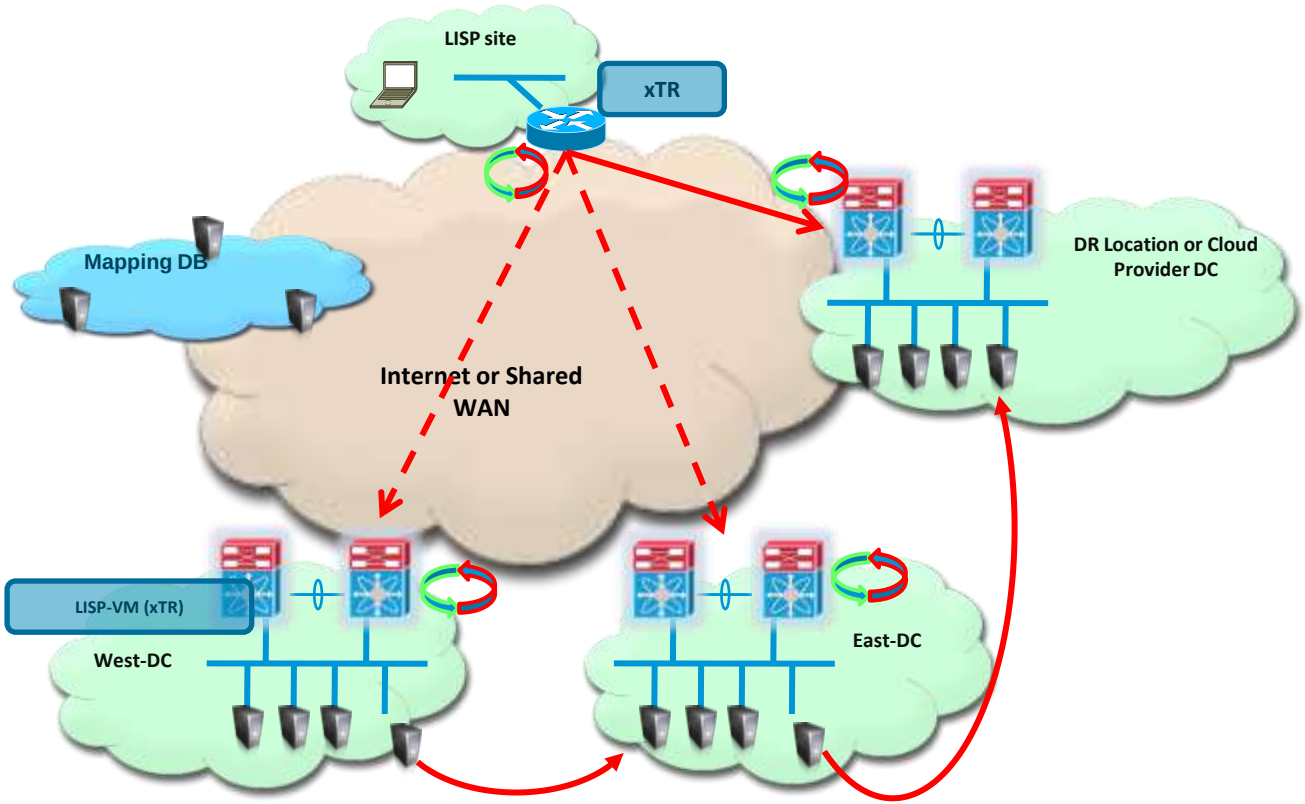
LISP – Data Plane
Session Persistency

- LISP nodes advertize locator policies through mapping system to adjacent nodes
- Session Persistency (beneficial for LISP Mobile nodes, VM Mobility, etc.)
- Optimized routing – avoids triangular routing



Virtual Machine Mobility

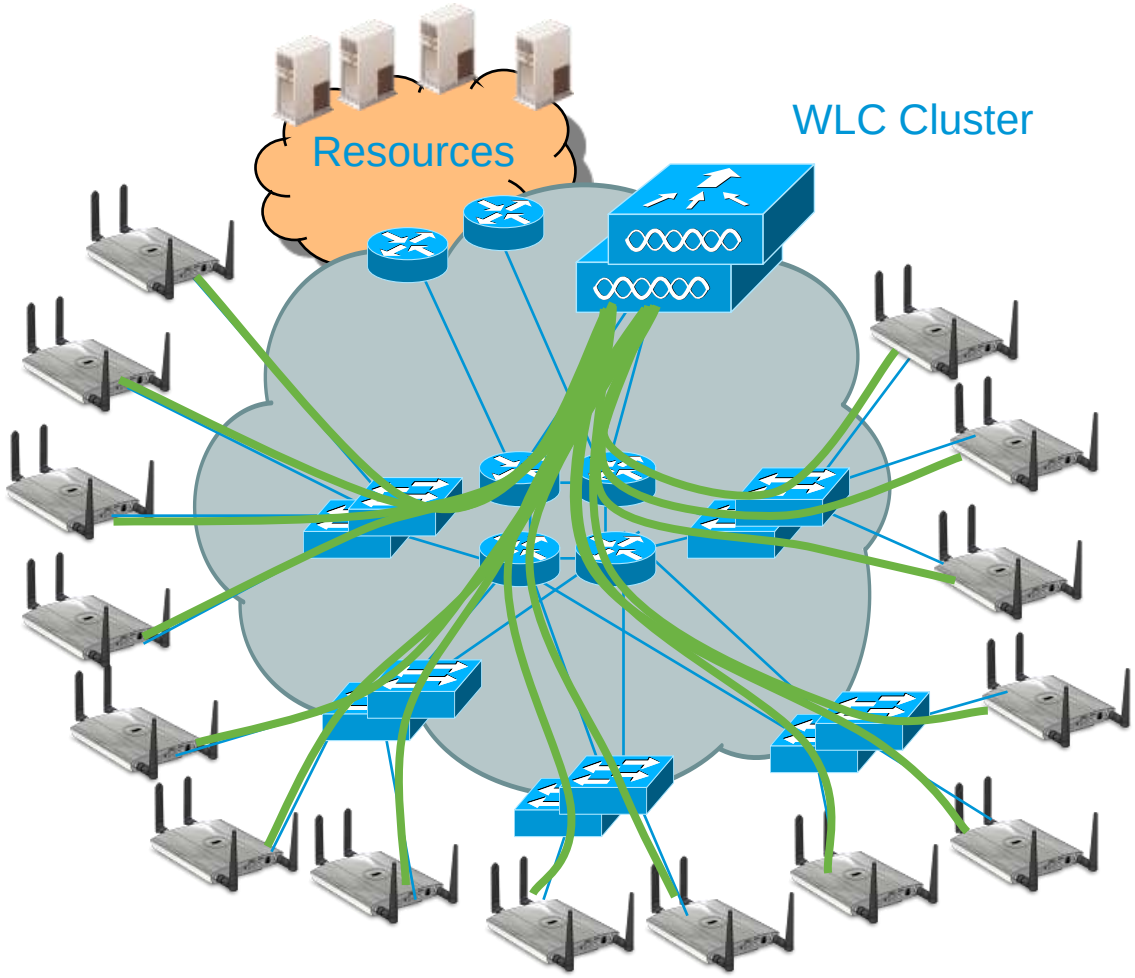
Session Persistency relevance to Data Centre



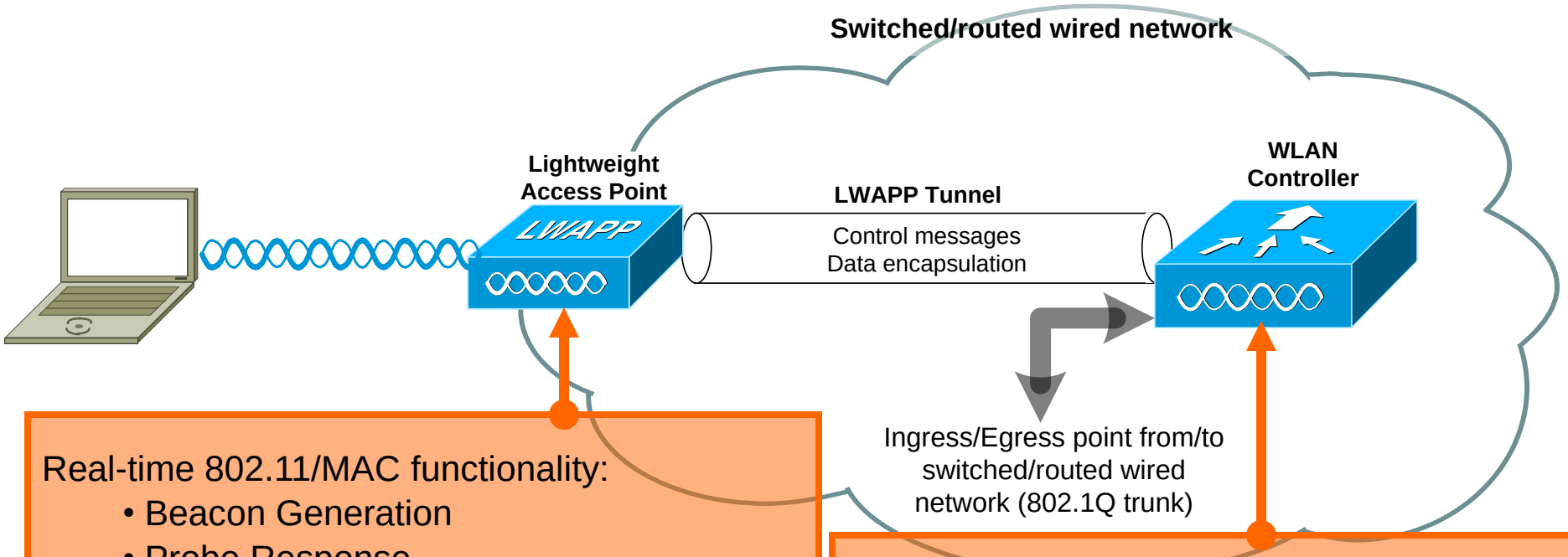
CAPWAPP

Network Anchor in the 802.11 environment

- LWAPP/CAPWAP Infrastructure bring an anchor point for the 802.11 networks



Division of Labor—Split MAC



Real-time 802.11/MAC functionality:

- Beacon Generation
- Probe Response
- Power management/Packet buffering
- 802.11e/WMM scheduling, queueing
- MAC layer data encryption/decryption
- 802.11 control messages

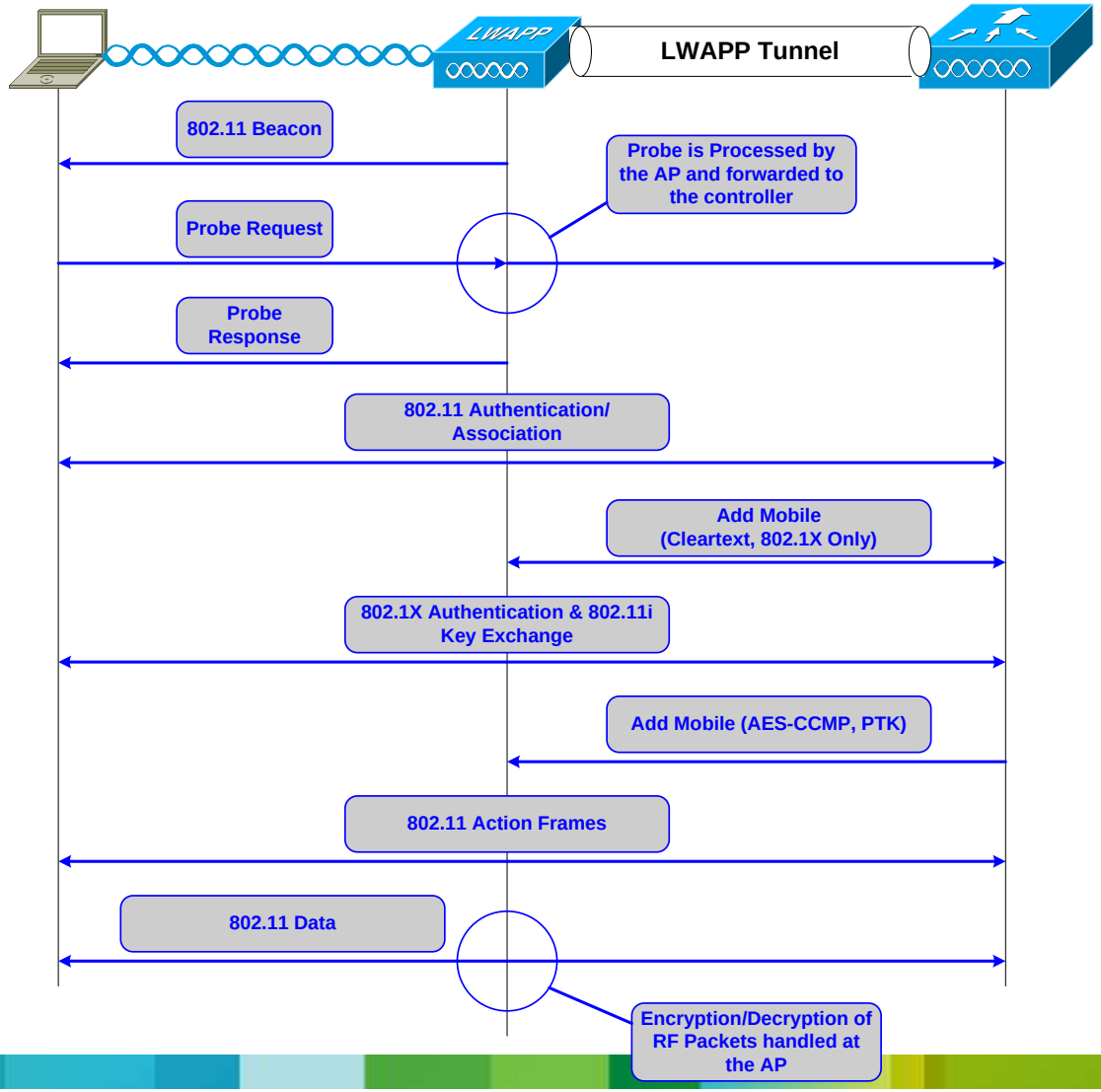
Data encapsulation/de-encapsulation
Fragmentation/De-fragmentation

Non real-time 802.11/MAC functionality:

- Assoc/Disassoc/Reassoc
- 802.11e/WMM resource reservation
- 802.1X/EAP
- Key management

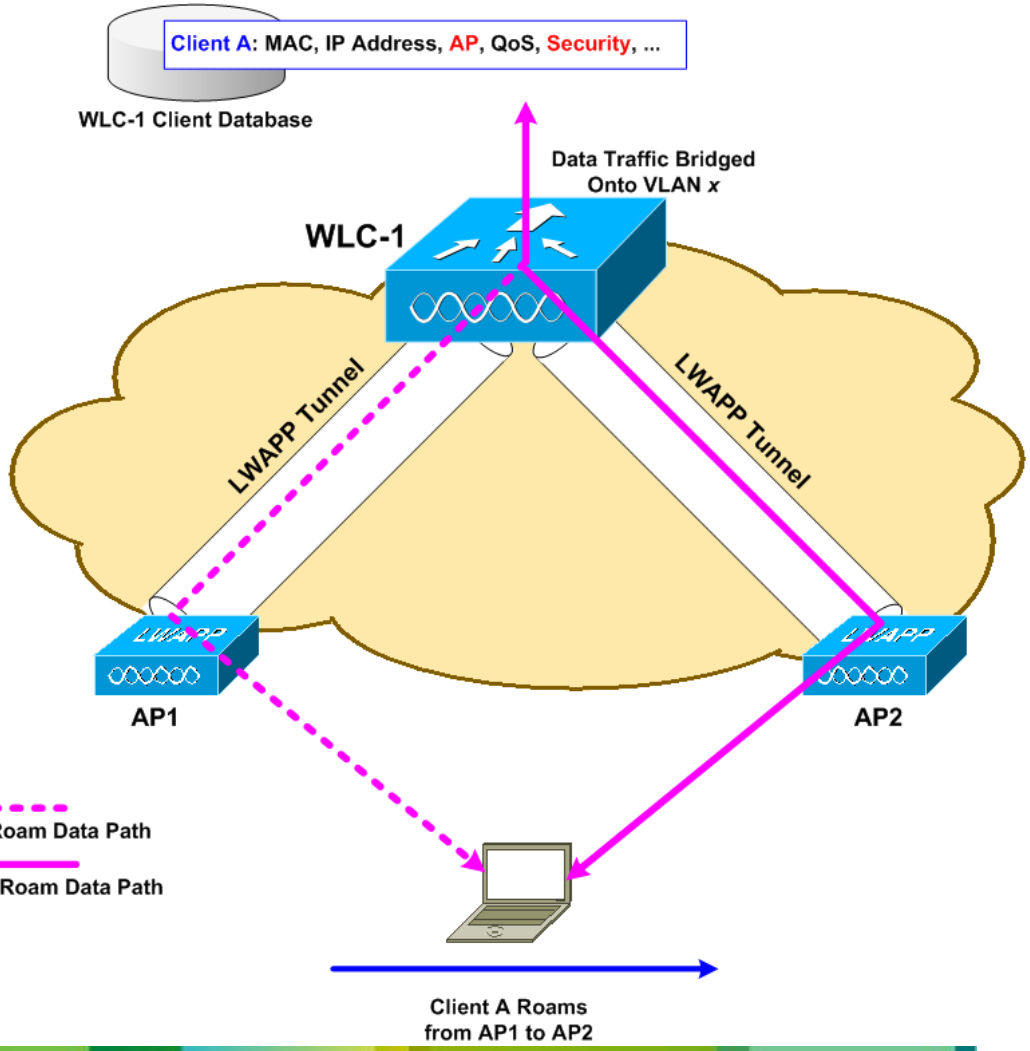
802.11 Distribution services
Wired/Wireless Integration services

Division of Labor—Split MAC Illustrated

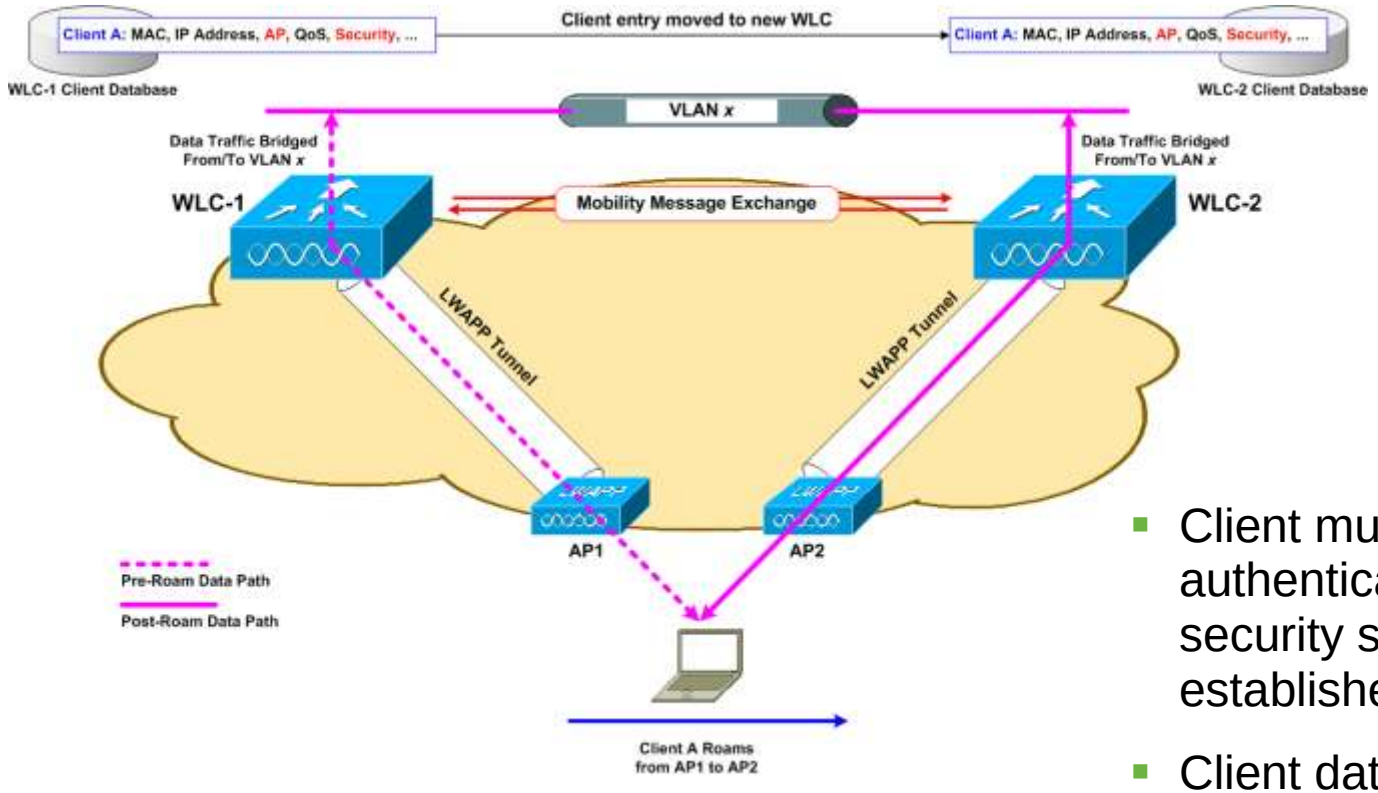


Intra-Controller Roaming

- Intra-Controller roam happens when an AP moves association between APs joined to the same controller
- Client must be re-authenticated and new security session established
- Controller updates client database entry with new AP and appropriate security context
- No IP address refresh needed



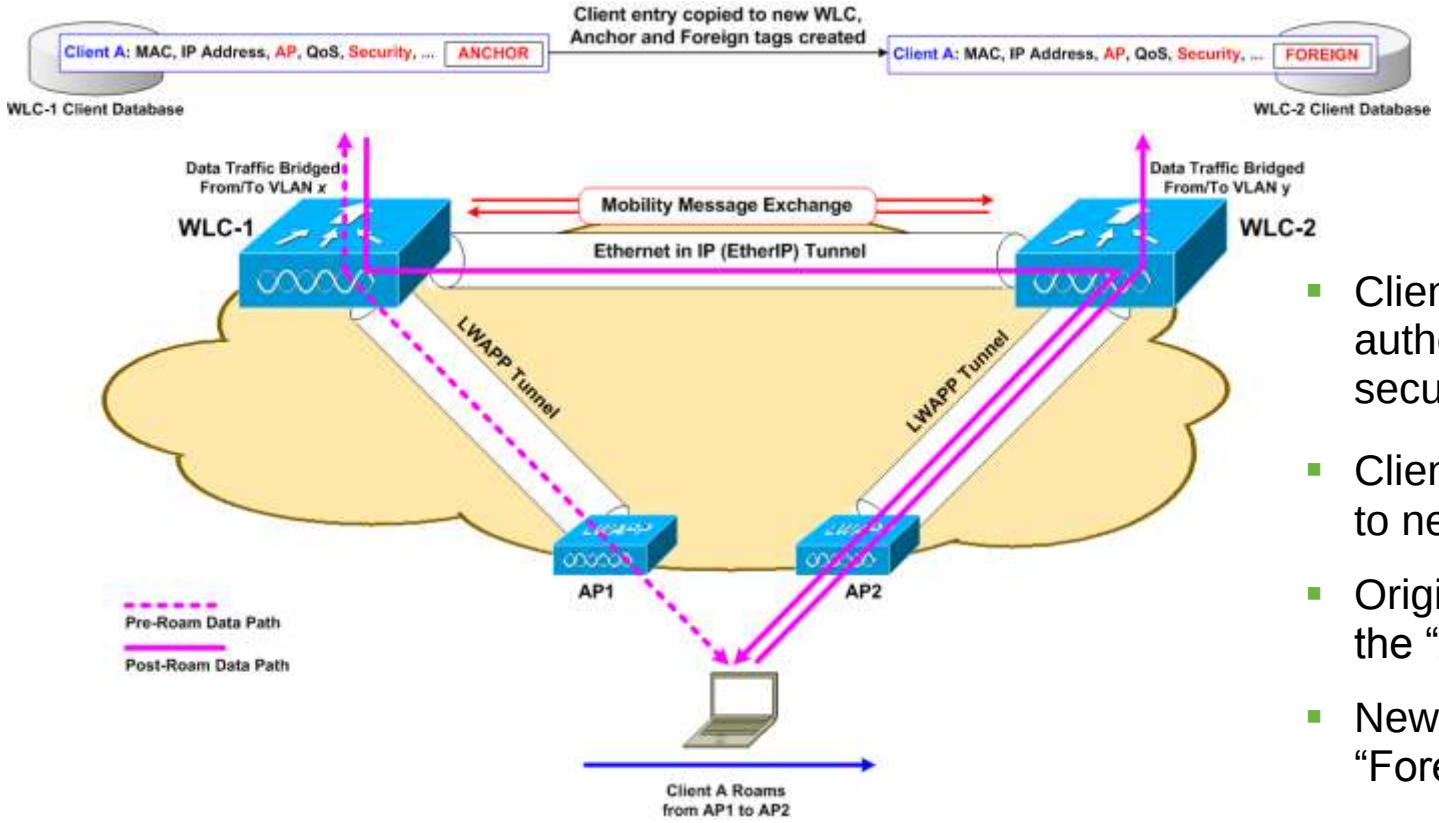
Layer-2 Roaming—Inter-Controller



- L2 Inter-Controller roam happens when an AP moves association between APs joined to the different controllers but client traffic bridged onto the same subnet

- Client must be re-authenticated and new security session established
- Client database entry moved to new controller
- No IP address refresh needed

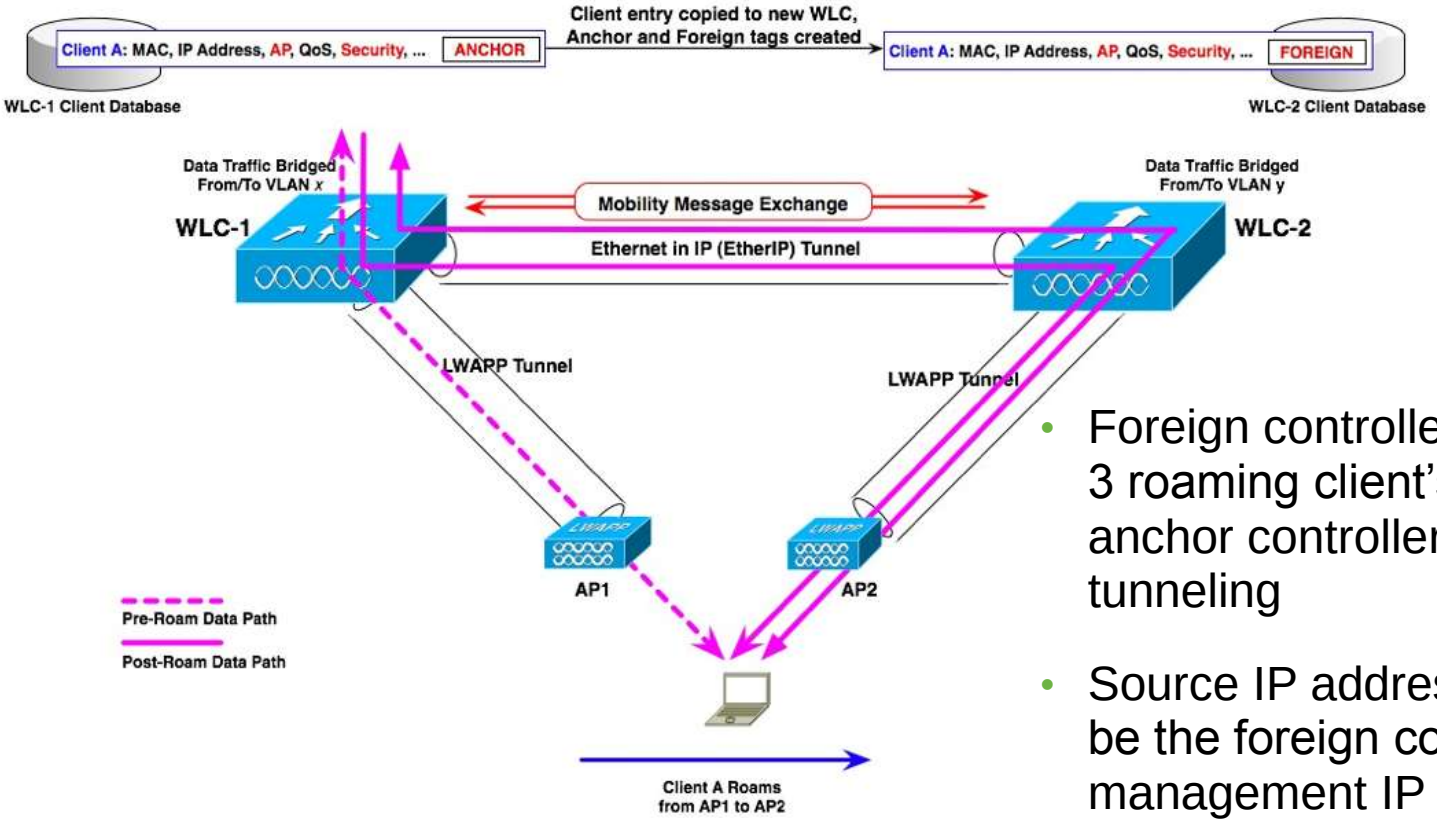
Layer-3 Roaming—Inter-controller



- Client must be re-authenticated and new security session established
- Client database entry copied to new controller
- Original controller tagged as the “Anchor”
- New controller tagged as the “Foreign”
- No IP address refresh needed
- Asymmetric traffic path established

- L3 Inter-Controller roam happens when an AP moves association between APs joined to the different controllers but client traffic bridged onto different subnet

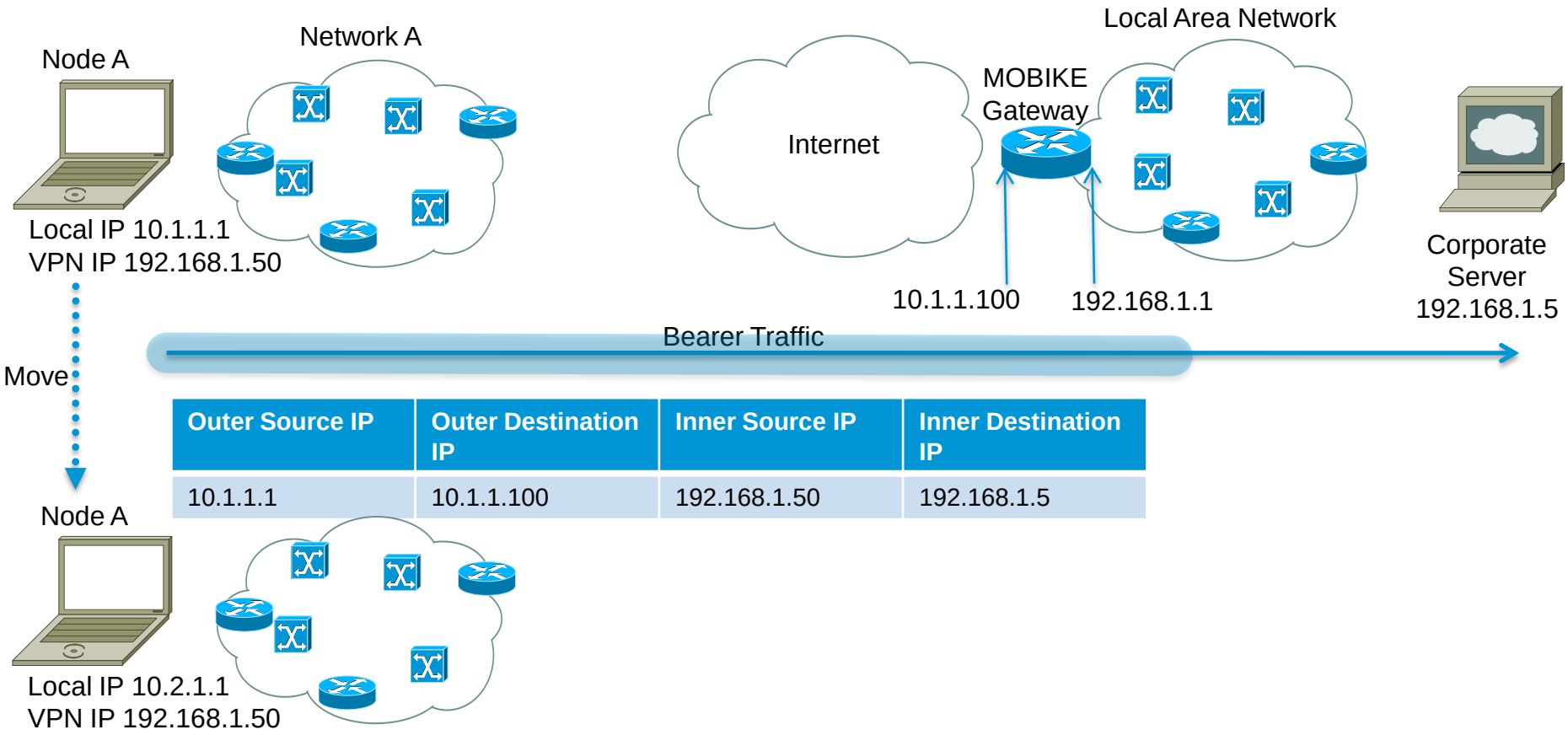
Layer-3 Roaming—Symmetric Mobility (4.1)



- Foreign controllers will send Layer 3 roaming client's packet back to its anchor controller through EtherIP tunneling
- Source IP address of the packet will be the foreign controller's management IP address
- Upstream routers that have Reverse Path Forwarding (RPF) will forward on packets
- Configurable option in software release 4.1

Mobike

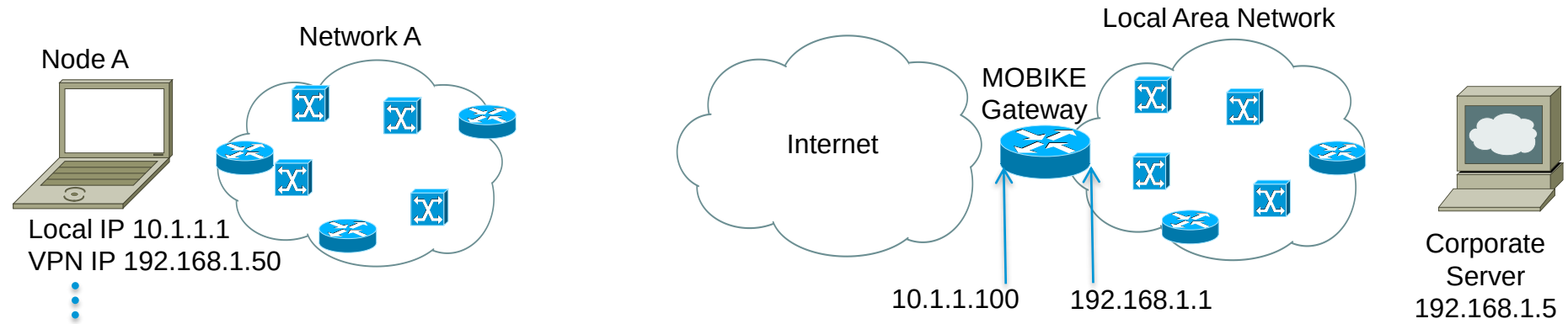
Maintaining VPN Session with MOBIKE



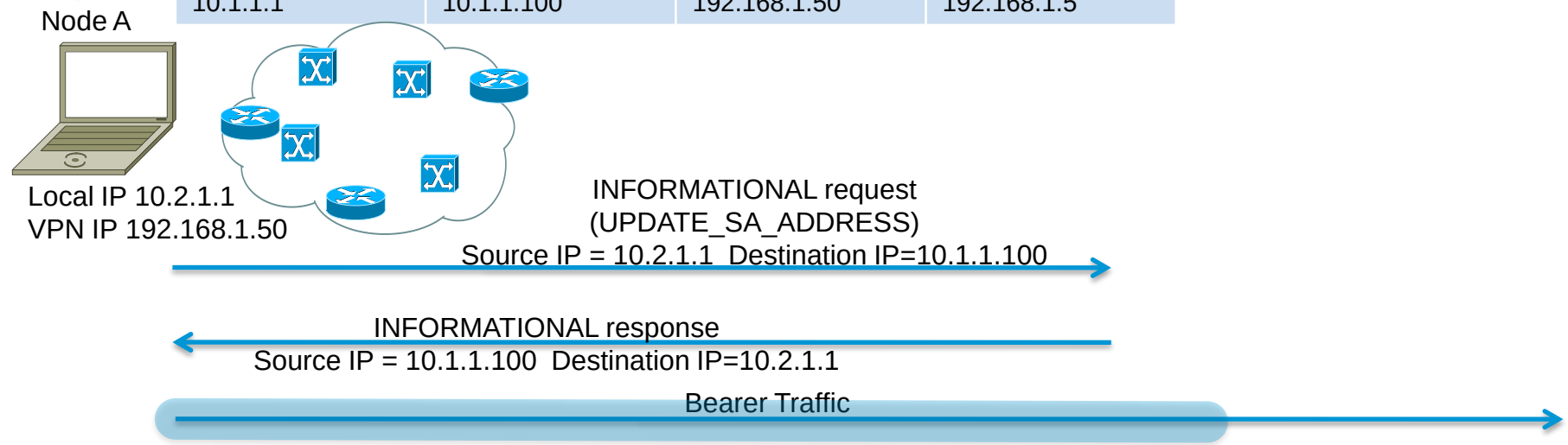
Outer Source IP	Outer Destination IP	Inner Source IP	Inner Destination IP
10.1.1.1	10.1.1.100	192.168.1.50	192.168.1.5

Outer Source IP	Outer Destination IP	Inner Source IP	Inner Destination IP
10.2.1.1	10.1.1.100	192.168.1.50	192.168.1.5

MOBIKE Call Flow



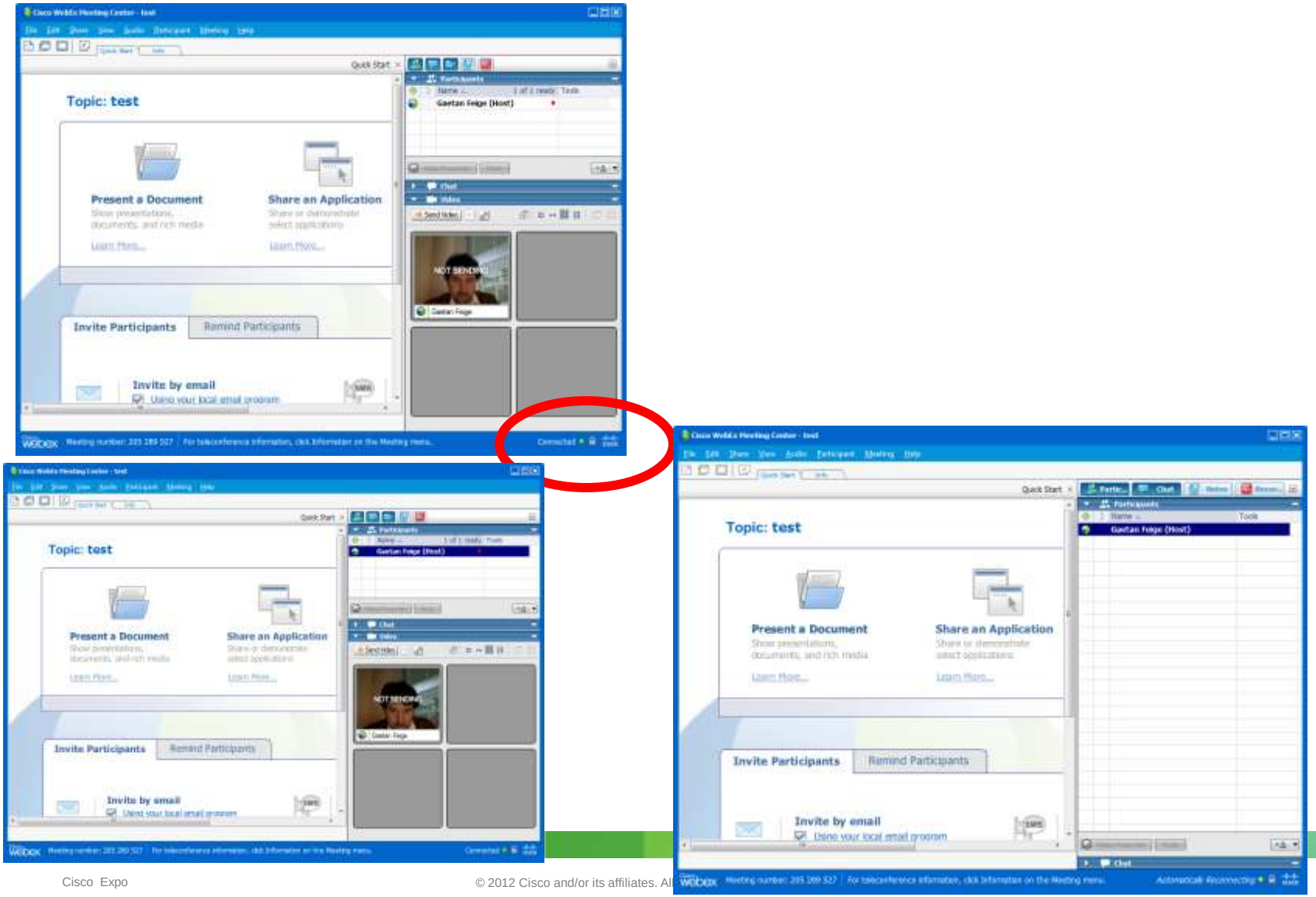
Outer Source IP	Outer Destination IP	Inner Source IP	Inner Destination IP
10.1.1.1	10.1.1.100	192.168.1.50	192.168.1.5



Outer Source IP	Outer Destination IP	Inner Source IP	Inner Destination IP
10.2.1.1	10.1.1.100	192.168.1.50	192.168.1.5

Application Layer

Webex SSL reconnect



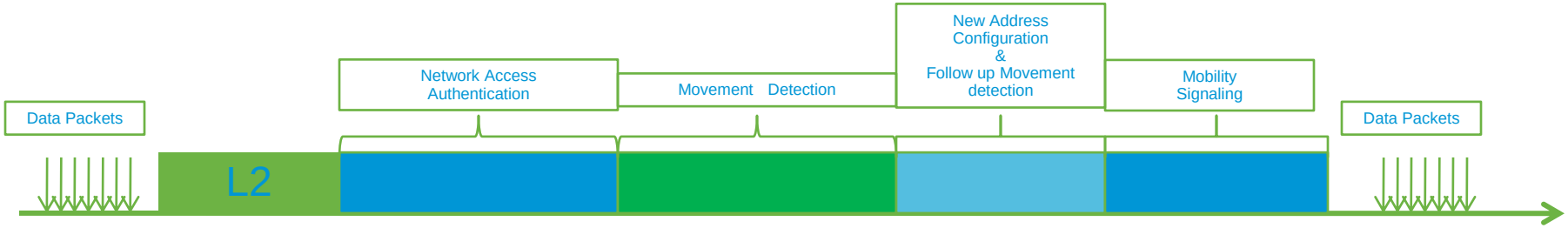
Video Solutions

- **MS Silverlight**
  - MediaElement.BufferingTime defaults to 5 seconds
  - smooth HD
- **Adobe Flash**

Other considerations

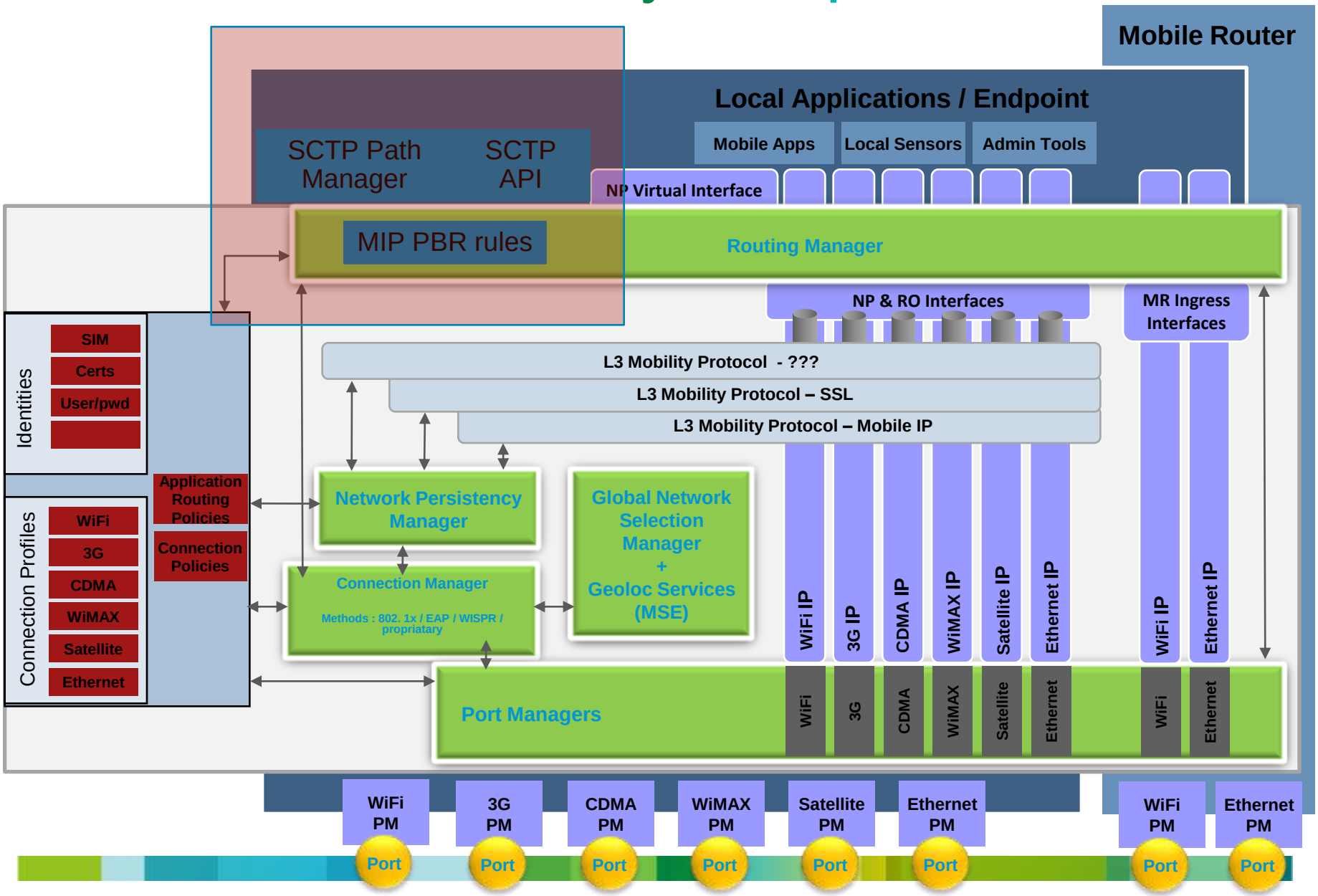
Handover Packet Loss vs Multiple Bearers

- The two causes for packet loss are:
  - A physical layer change disrupting layer 1 communication
    - change of a radio frequency
  - A logical mismatch between a MN and a CN
    - time to acquire a new IP address, if no other available
    - change of a tunnel endpoint IP address and duration to logically rebuild the tunnel
    - propagation time for the update message to reach the other side



- Single versus multiple bearers
  - Packet loss is unavoidable when using a single bearer due to physics change
    - Buffering and forwarding buffered packets is the only choice
  - Using multiple bearers can allow zero packet loss if anticipating layer 2 disruptions

Client Based Mobility – Impact on Clients

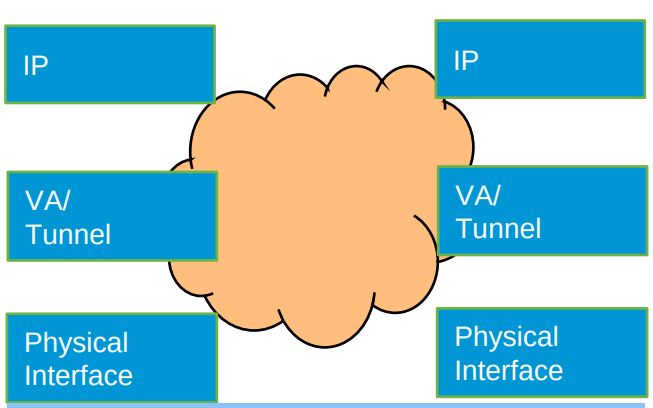


End2End Mobility vs Secure Handover

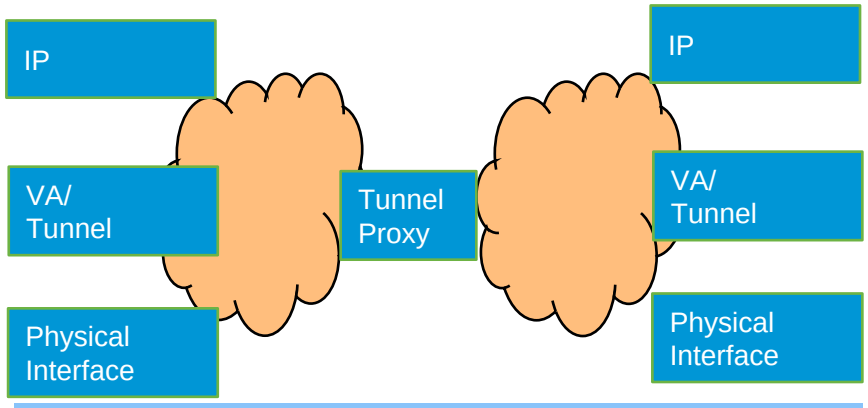
- End2End mobility requires both MN & CN to support a security association for IP address change in order to protect against Man-in-the-Middle attacks. Not all the End2End mobility protocols are secure in that sense.
- Register a new IP address
  - GTP
  - MIPv4: RRQ
  - MIPv6: BU
  - SCTP: Add address
  - Multipath TCP: Add address
- Secure the registration of a new IP address
  - MIPv4: weak authentication (based on HMAC-MD5 hash)
  - MIPv6: based on IPSEC/IKEv2
  - DSMIPv6: based on IPSec/IKEv2
  - SCTP: requires security, RFC negates shared key and negotiated key. Private/Public key best.
  - Multipath TCP: requires some security, mechanisms open

Mobility & Location privacy

- End2End mobility allows a CN to know of any IP address change from the MN.
- IP addresses can be used to know your location:
- http://whatismyipaddress.com/
- In some cases, users do not want to allow a third party to track a user's location without their permission
- A change in IP address which is visible to a correspondent node can be used to infer a change in location



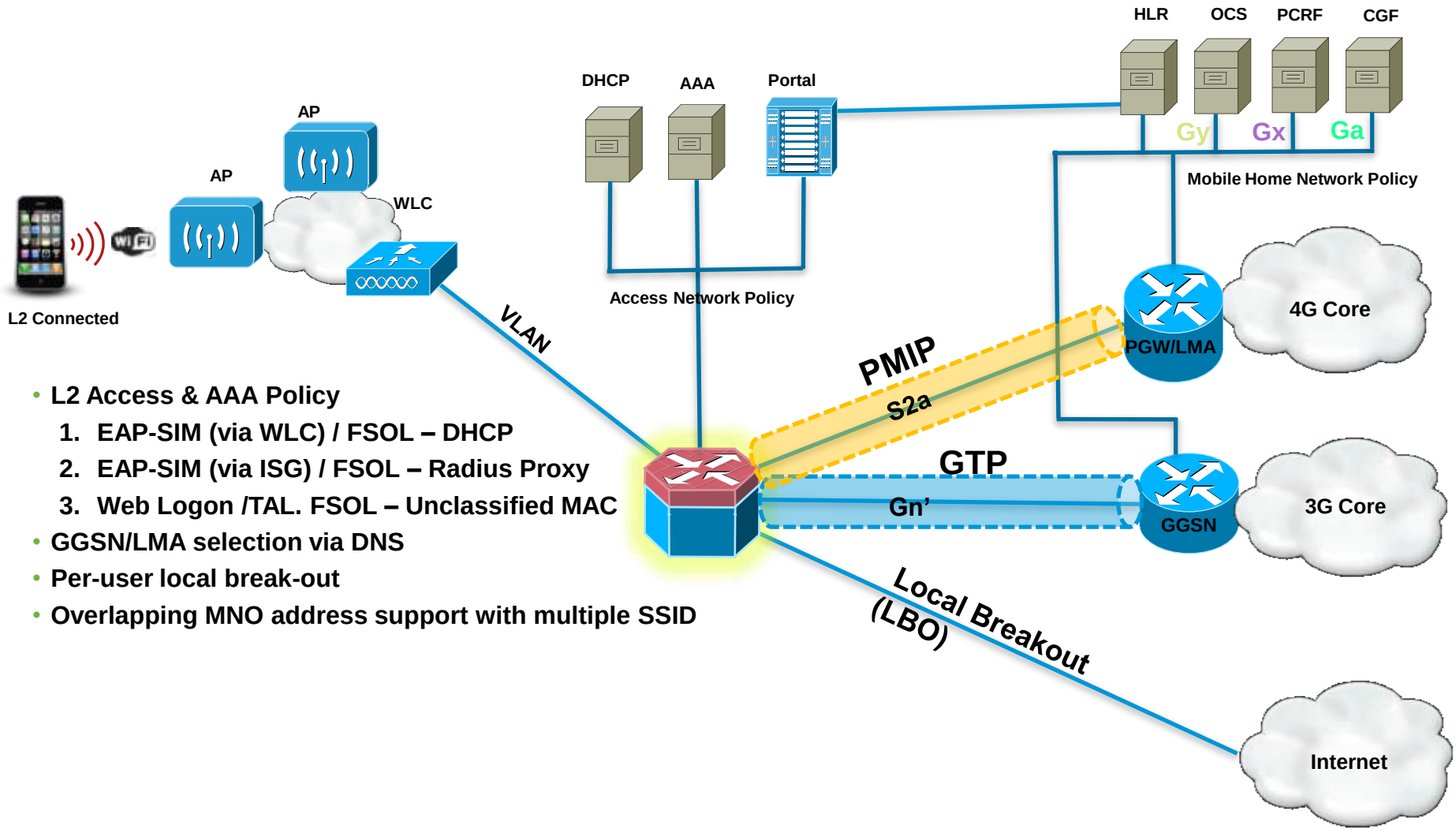
E2E Tunnel/Visibility



Concealed Location/Mobility

Closing

Maintaining session persistency WiFi – 3G/4G (example of architecture)



- L2 Access & AAA Policy
  1. EAP-SIM (via WLC) / FSOL – DHCP
  2. EAP-SIM (via ISG) / FSOL – Radius Proxy
  3. Web Logon /TAL. FSOL – Unclassified MAC
- GGSN/LMA selection via DNS
- Per-user local break-out
- Overlapping MNO address support with multiple SSID

Thank you.