Integration of 802.11 and Third-Generation Wireless Data Networks

Milind M. Buddhikot
mbuddhikot@bell-labs.com
Center for Networking Research
Lucent Bell Labs Research

Lucent Technologies
Bell Labs Innovations

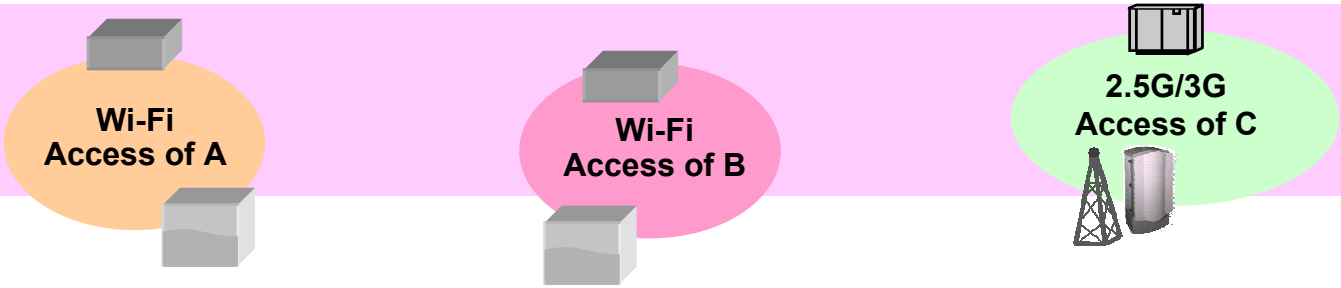
Outline

- Current Trends and Rationale for Integration
- Integration of 802.11 and 3G
  - Integration approaches
    - Tight
    - Loose
  - A Prototype Implementation
    - IOTA Gateway
    - Multi-interface client
    - Measurements
- Conclusions

Evolving Picture

- 3G1X, 3G1XEVDO, UMTS, 802.11a/b access operated by *different providers*
- Customers with multi-radio capable end devices
- Multitudes of applications, seamless roaming, preserve sessions, single bill

Wireless Access Networks



Subscriber Service

One bill from
One provider (3G carrier?)

Roaming or even
Seamless Handoff
in Multiple Networks

Uninterrupted Applications:
Streaming, Email, Corporate VPN, Web

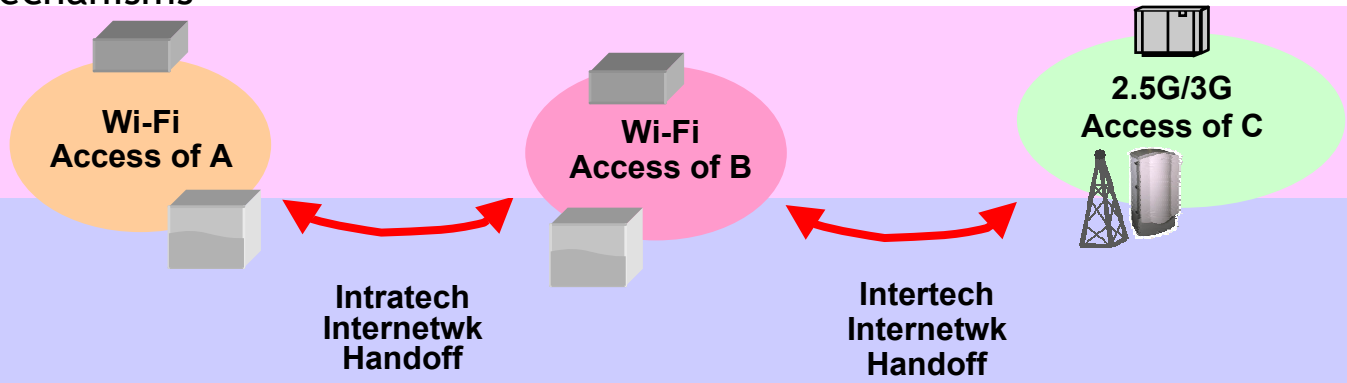
Terminal Possibilities

Evolving Picture

- **Seamless roaming:**
  - Efficient authentication
  - inter and intra-tech handoffs via Interoperation of mobility mechanisms
- Billing info across access networks and providers
- Uniform service mapping
- Roaming Agreements!

Wireless Access Networks

Handoff Possibilities



Subscriber Service

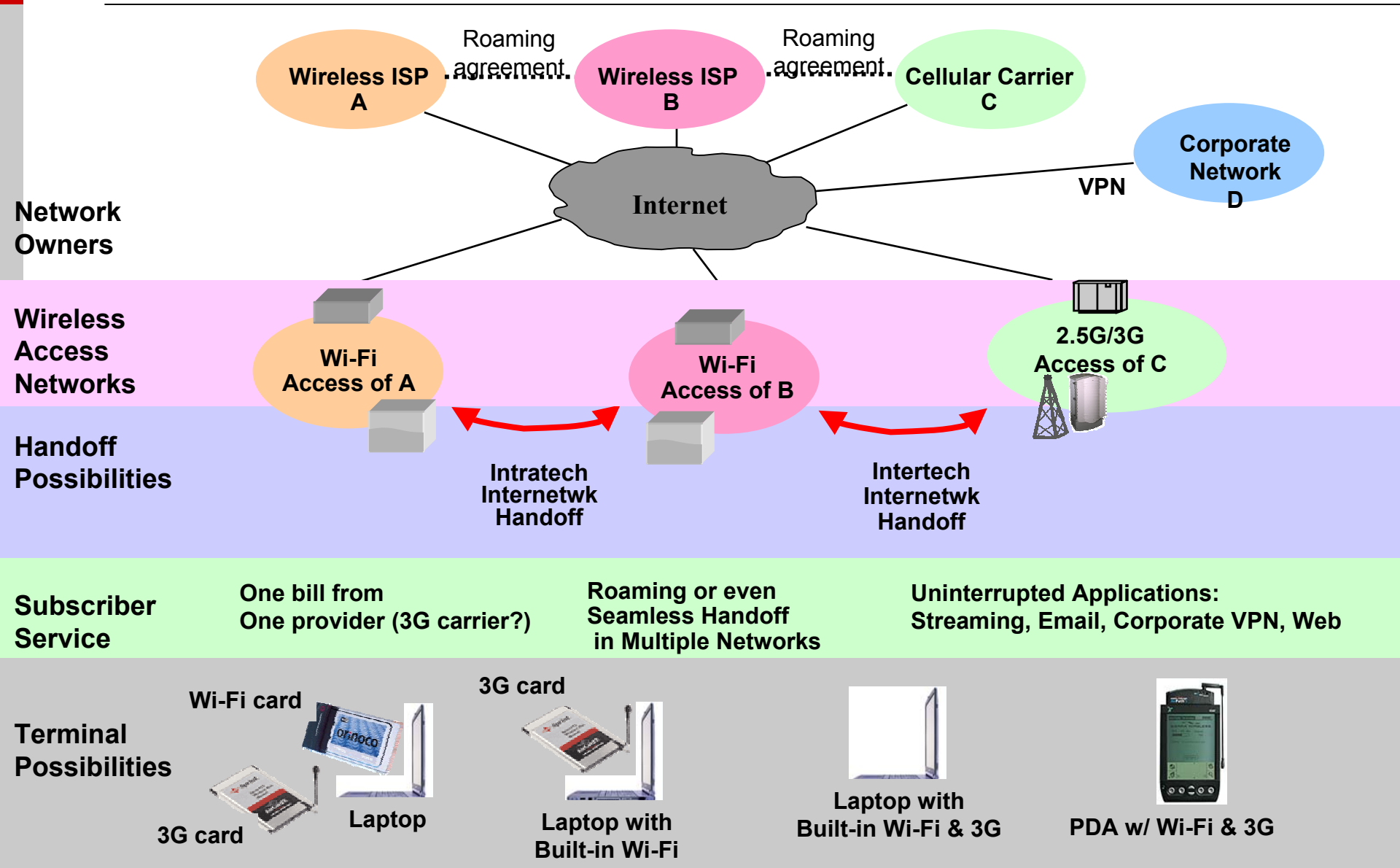
One bill from
One provider (3G carrier?)

Roaming or even
Seamless Handoff
in Multiple Networks

Uninterrupted Applications:
Streaming, Email, Corporate VPN, Web

Terminal Possibilities

Complete Picture

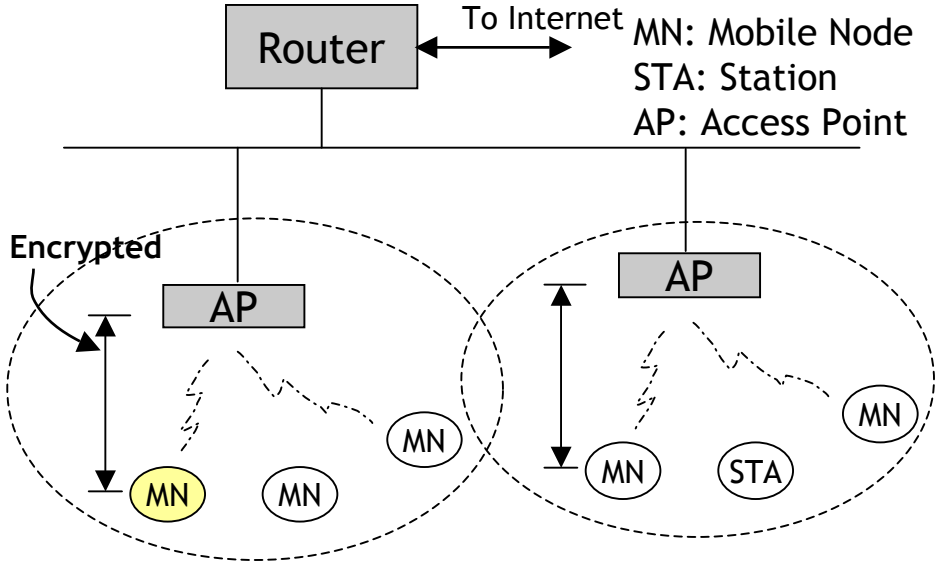


Integration Architectures

- Tight and Loose

Lucent Technologies
Bell Labs Innovations

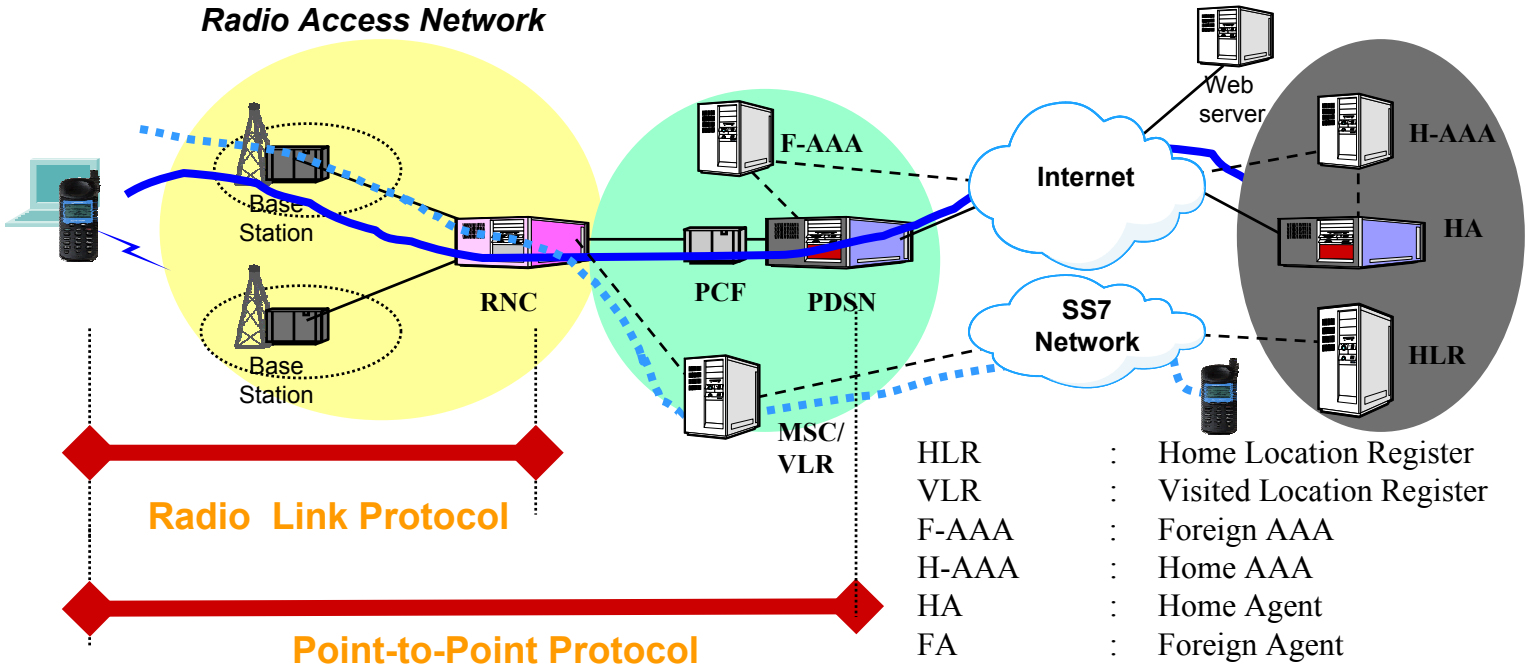
802.11b Network



- **Infrastructure mode:**
  - MNs communicate via base stations Access Points (AP)
  - AP s together with Ethernet characterized by ESSID
  - 11-54 Mbps, Range limited 300-500m

- MN-AP communication encrypted using **WEP**
- Encryption keys may be established
  - Statically
  - Dynamically using 802.1x
    - With TKIP
- Layer-2 mobility via inter-AP protocols

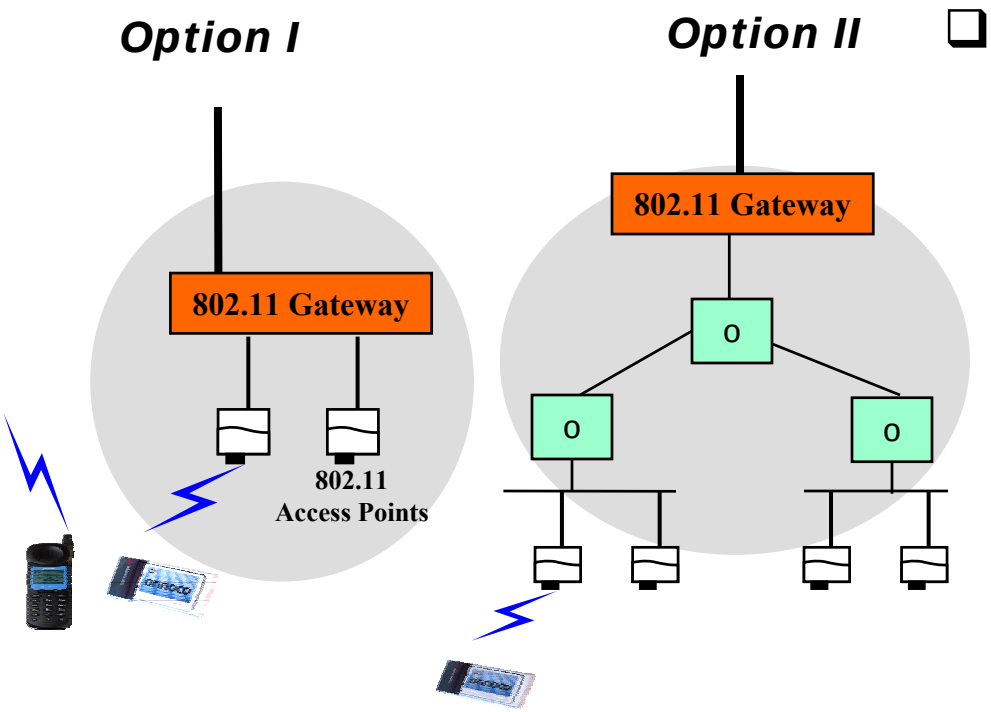
Representative 3G Network: CDMA2000 1X-RTT



HLR	:	Home Location Register
VLR	:	Visited Location Register
F-AAA	:	Foreign AAA
H-AAA	:	Home AAA
HA	:	Home Agent
FA	:	Foreign Agent
PDSN	:	Packet Data Serving Node
PCF	:	Packet Control Function
RNC	:	Radio Network Control

- 144 Kbps per carrier
- MN maintains
  - RLP connection to RNC
  - PPP connection to PDSN
- PDSN supports Mobile-IP and Simple-IP mode
  - FA functions in MIP mode

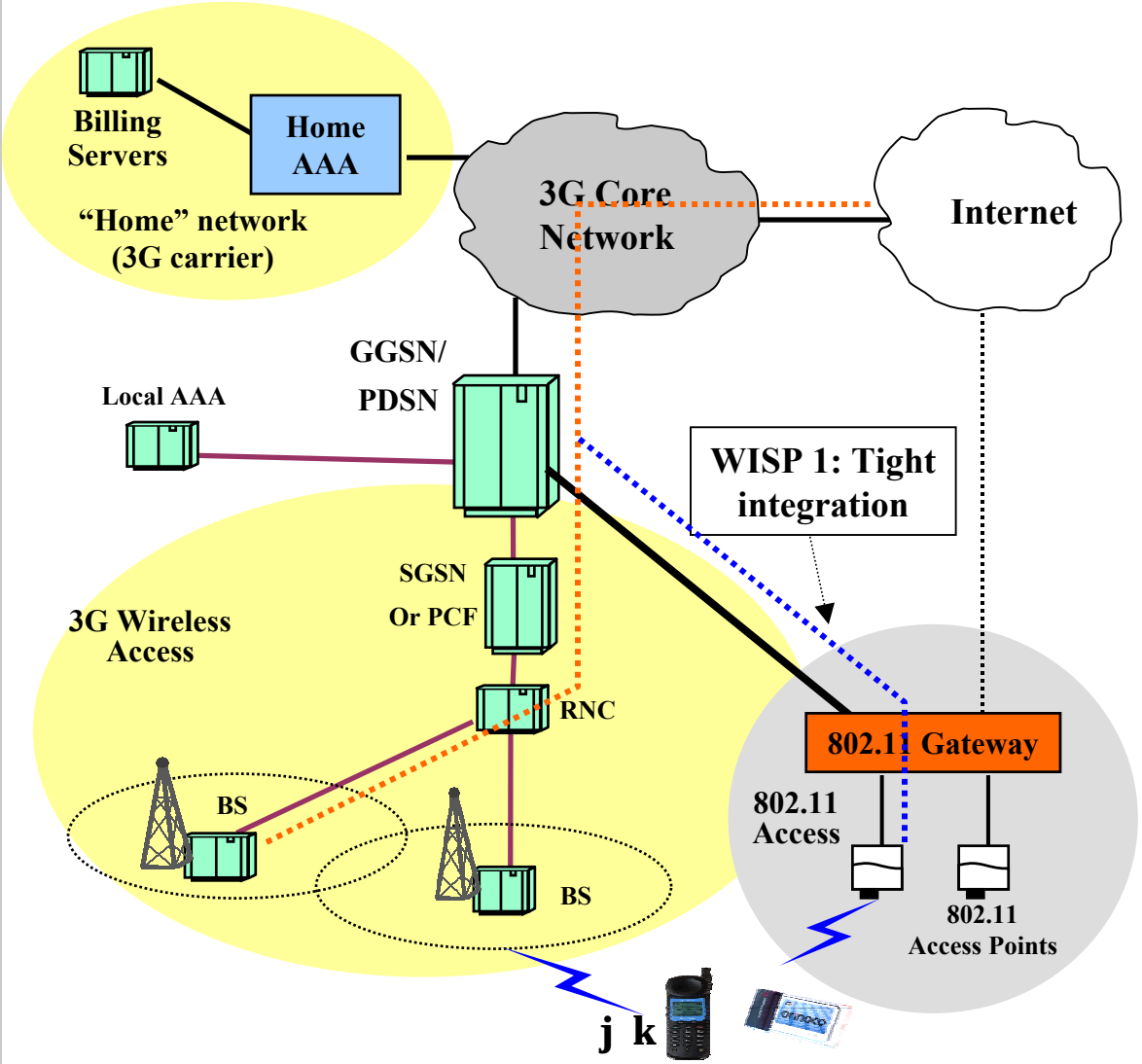
Basic Ideas for Integration



- Both integration approaches use a new network element called ***802.11 Gateway***
  - Deployed in the 802.11 network

- Observations:
  - Multiple 802.11 access points connect to the gateway
  - **Option I:** A gateway per subnet, each with multiple 802.11 AP s
  - **Option II:** One gateway per routed network with multiple subnets
  - Can perform layer-2, 3, 4, 7 packet processing
  - Functionality, protocol support depends on the integration approach

Tight Integration



- 802.11 gateway uplink connects to the to 3G core network
  - Connect to GGSN in UMTS or PDSN in 3GPP2
  - Uplink is ATM over T1, T3, or SONET
  - Ethernet, POS with IP Release 6 of UMTS.
- Gateway appears as a ***new SGSN or PCF***

Tight Integration (contd.)

- **Goal:** Use the 3G protocol stack on the MN to sign on and use 802.11 networks
  - 802.11 RADIO is yet another 3G radio
- **Advantages:**
  - Requires minimal changes to the client (in theory)
  - Use same authentication infrastructure and profile
  - Easy to generate one common billing statement
  - Easy to view 802.11 network from the network management point

→ **Disadvantages far outweigh the above**

Disadvantages of Tight Integration

- **Traffic engineering:**
  - Wide area cellular core networks carefully engineered to handle (peak) traffic from base stations
  - Since, 802.11 traffic to the internet flows over the 3G core network, traffic load increased by ~25 to 100 times
  - Core network must be re-engineered else QoS for regular 3G traffic severely affected
- **Authentication overhead**
  - Use of 3G authentication scheme requires gateway interface to a VLR or implement VLR functions
  - Ciphering, Integrity keys in 3G may not be usable in a 802.11 encryption procedure
  - **Split implementation complicates gateway**
    - MN to Gateway protocol: EAP over RADIUS
    - Gateway to VLR/HLR: 3G protocol

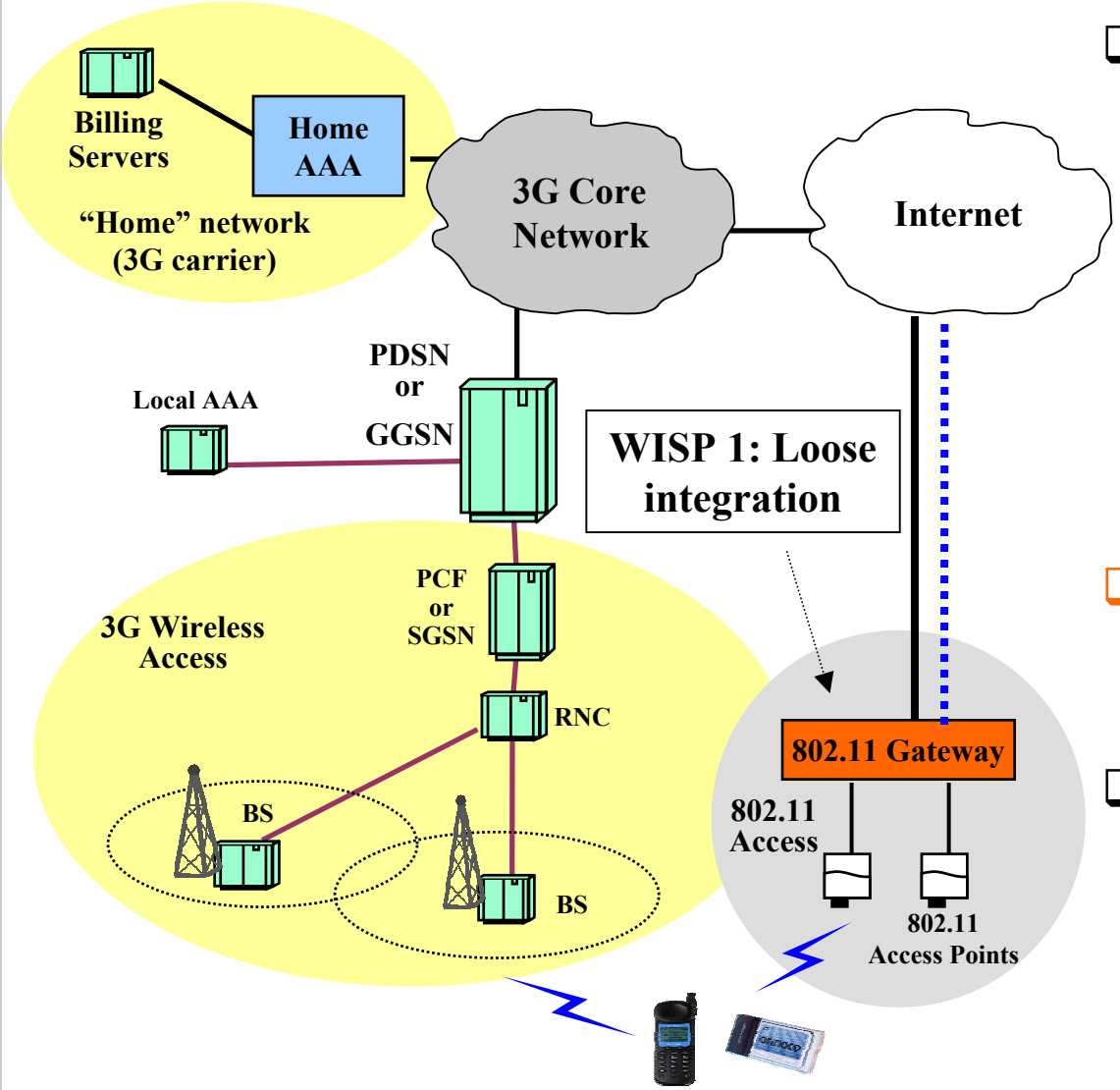
Client overheads for Tight Integration

- Client software must
  - include 3G stack even for 802.11 only users
  - Use SIM Card on 802.11 network
  - Must use appropriate 802.1x signaling packets to transport 3G specific signaling traffic
    - Involves client changes , definition of new EAP types
- 3G software not usable transparently
  - Additional glue software required to hide 802.11 and 802.1x specific differences from 3G software

Provider Nightmare

- 802.11 infrastructure must be owned by 3G provider
  - 3G provider burdened with rollout of 3G and 802.11!
- Else, if 802.11 network operated by other provider
  - Alternate internet uplink for non-3G roaming customers
- If 802.11 provider wants roaming agreement with multiple 3G providers it must have at least one uplink per provider!
  - Provider cores are non-overlapping
- Wireless carrier cannot benefit from 802.11 Wireless ISP deployments
  - 802.11 networks not deployed independently of GPRS/UMTS
- Gateway complicated for co-existing non-3G and 3G-roaming customers
  - QoS mapping from UMTS to 802.11e for roaming 3G customers
  - SS7 awareness for authentication

Loose Integration Architecture

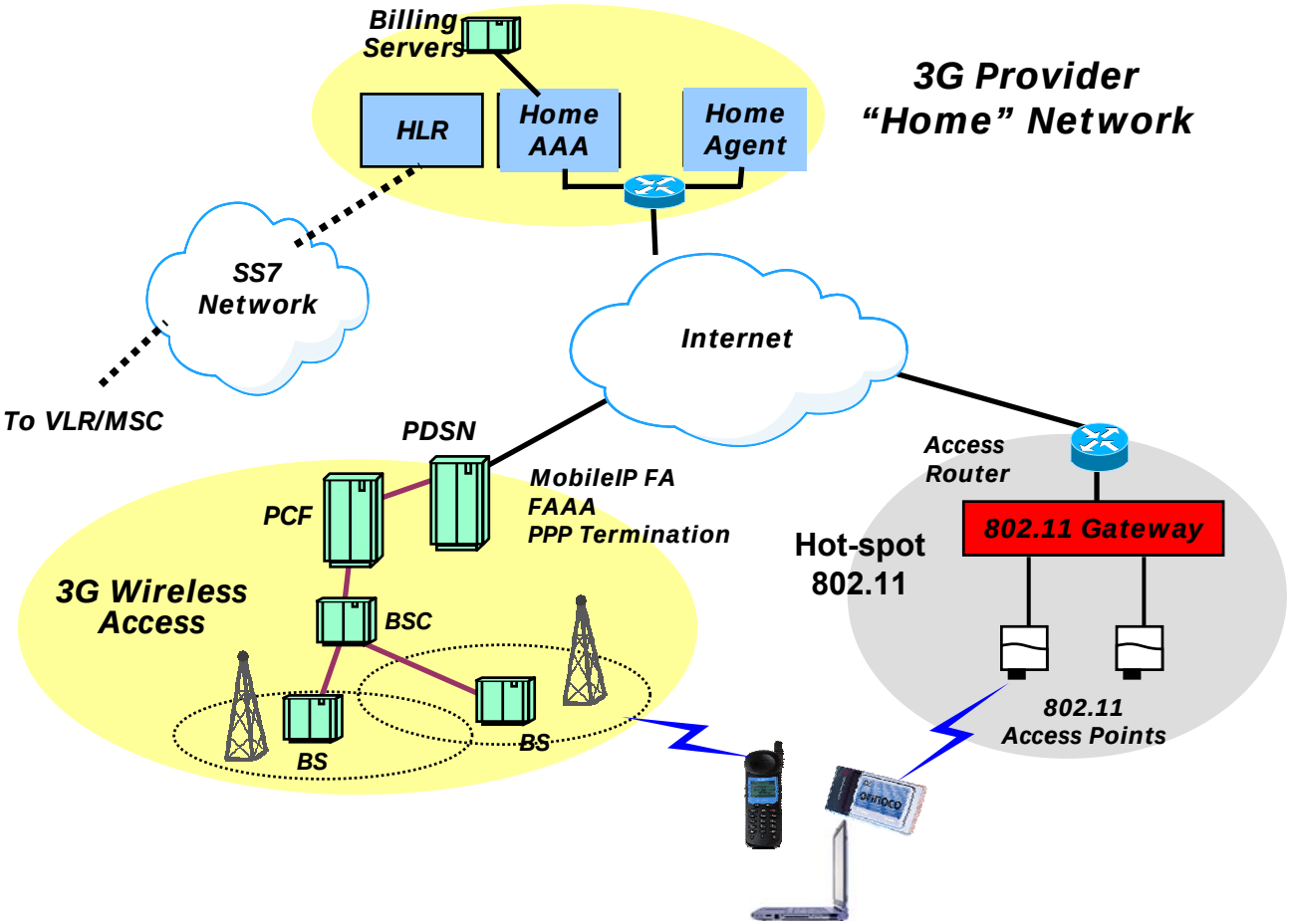


- 802.11 gateway connected to the internet via uplink
  - Option I or II mode
  - Layer-2 or layer-3 connection
  - No direct connectivity to 3G core network
- **Loose:** Data paths for two networks completely separated
- 802.11 network can be owned by different provider
  - Roaming contract with 3G provider

Loose Integration

- 802.11 provider authenticates the 3G roaming customer using 3G credentials
  - Roaming agreement with 3G provider which allows authentication traffic to be directed to 3G AAA/HLR
  - 3G provider may have to support new authentntication schemes as a part of roaming agreement
    - E.g.: SKE, TLS, SRP
- 802.11/802.1x keys can be derived as an outcome of authentication protocol
- Billing records generated by the gateway shipped to 3G HLR/H-AAA
  - Revenue settlement at a later date

Loosely Coupled 802.11 Integration with CDMA2000



- **Integration possible without changing 3GPP2 standards**
  - Integration based on MobileIP and AAA/RADIUS protocols
- **Same "Layer 3" Authentication on both 802.11 and CDMA2000 Networks**
  - Normal "Layer 2" authentication to HLR on CDMA2000 network

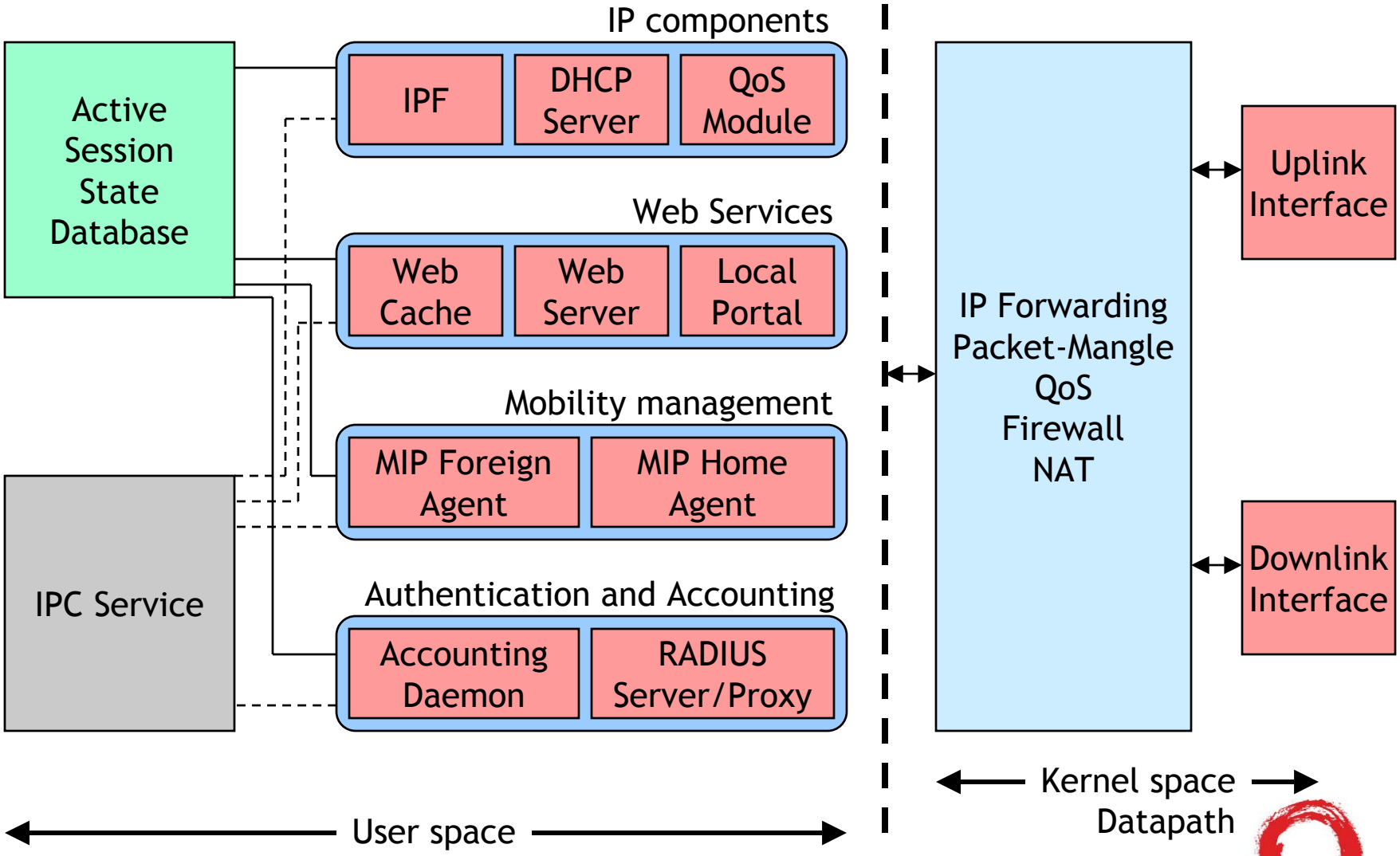
IOTA: A Prototype Implementation

Lucent Technologies
Bell Labs Innovations

The IOTA prototype

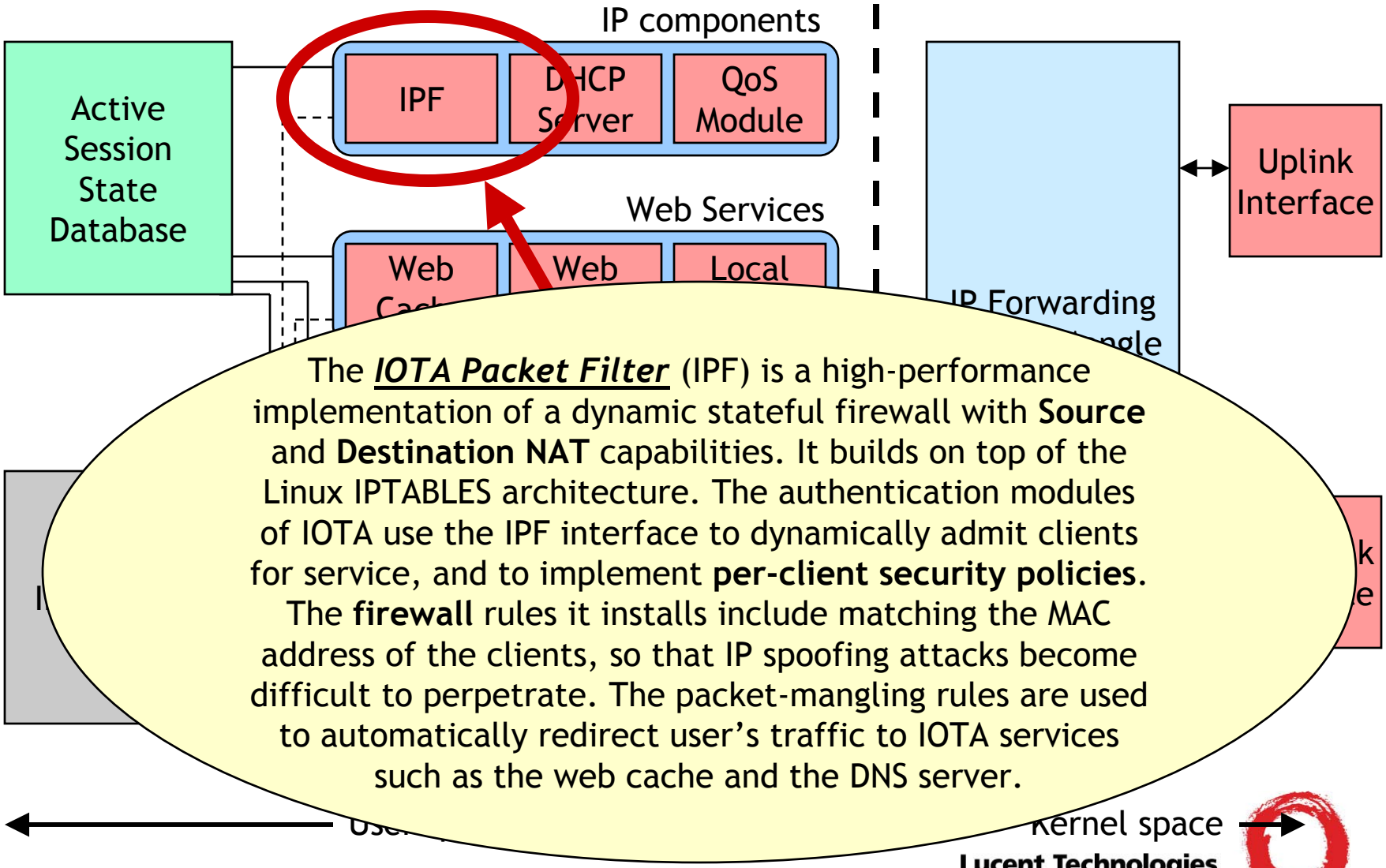
- IOTA=Integration Of Two Access technologies
  - 802.11b and 1XRTT, 1XEV-DO networks
- Research prototype that implements the loosely-coupled architecture
- Highly modularized IOTA gateway
  - Runs on off-shelf hardware (single/dual processor 750 MHz, Linux OS)
- Multi-interface mobility client software,
  - Management of mobility across multiple network interfaces and multiple wireless/wireline technologies

Software architecture of the IOTA gateway



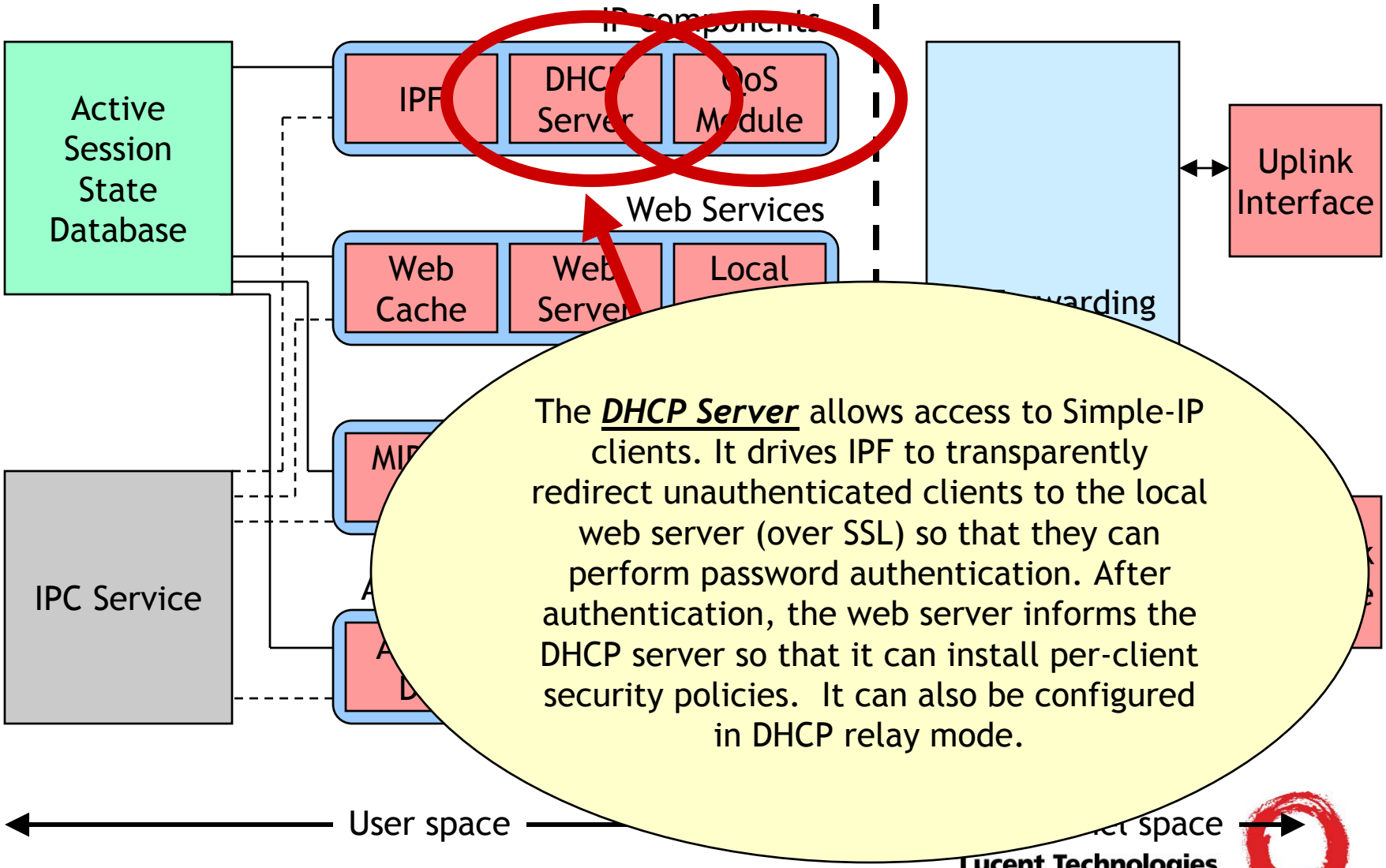
Lucent Technologies
Bell Labs Innovations

Software architecture of the IOTA gateway



The ***IOTA Packet Filter*** (IPF) is a high-performance implementation of a dynamic stateful firewall with **Source** and **Destination NAT** capabilities. It builds on top of the Linux IPTABLES architecture. The authentication modules of IOTA use the IPF interface to dynamically admit clients for service, and to implement **per-client security policies**. The **firewall** rules it installs include matching the MAC address of the clients, so that IP spoofing attacks become difficult to perpetrate. The packet-mangling rules are used to automatically redirect user's traffic to IOTA services such as the web cache and the DNS server.

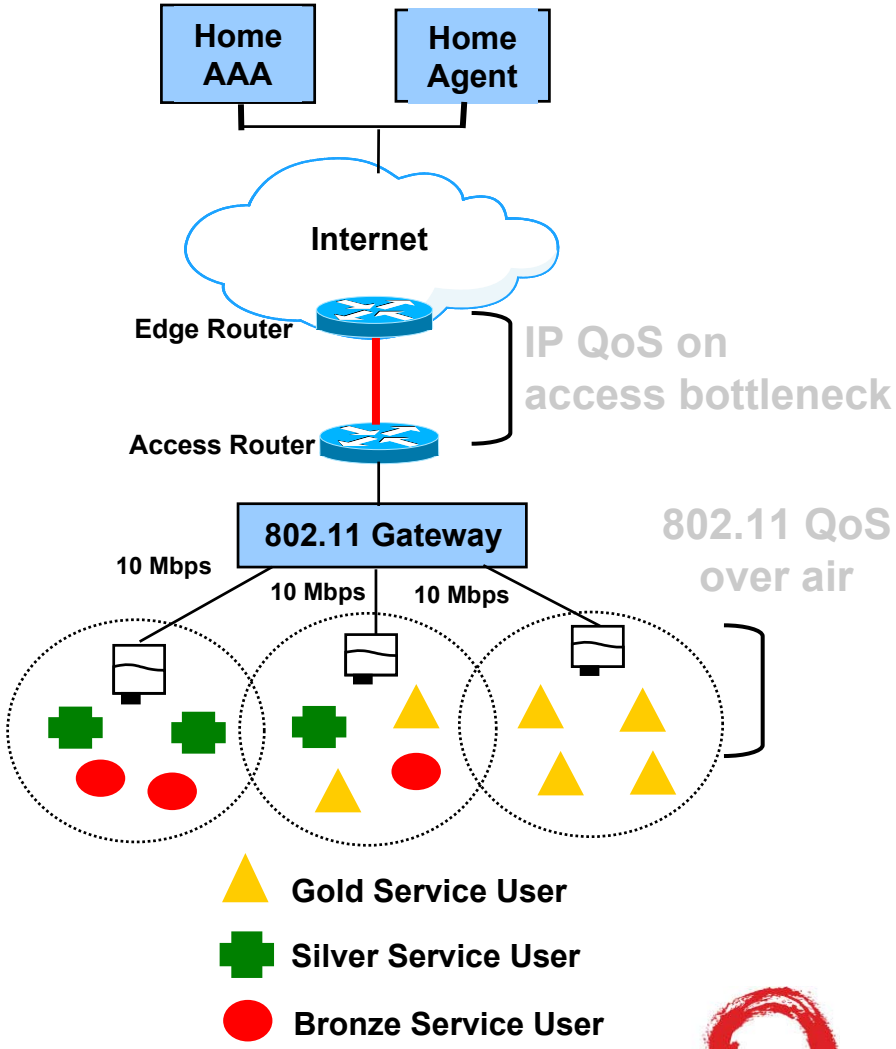
Software architecture of the IOTA gateway



The ***DHCP Server*** allows access to Simple-IP clients. It drives IPF to transparently redirect unauthenticated clients to the local web server (over SSL) so that they can perform password authentication. After authentication, the web server informs the DHCP server so that it can install per-client security policies. It can also be configured in DHCP relay mode.

QoS Features for 802.11

- Need QoS functionality in two spots of possible congestion
  - IP QoS on oversubscribed access link
  - QoS for 802.11 air interface
- 802.11e defining layer-2 QoS on the air-interface
- Layer-7/4/3 mechanisms for IP level QoS mechanisms complement 802.11e

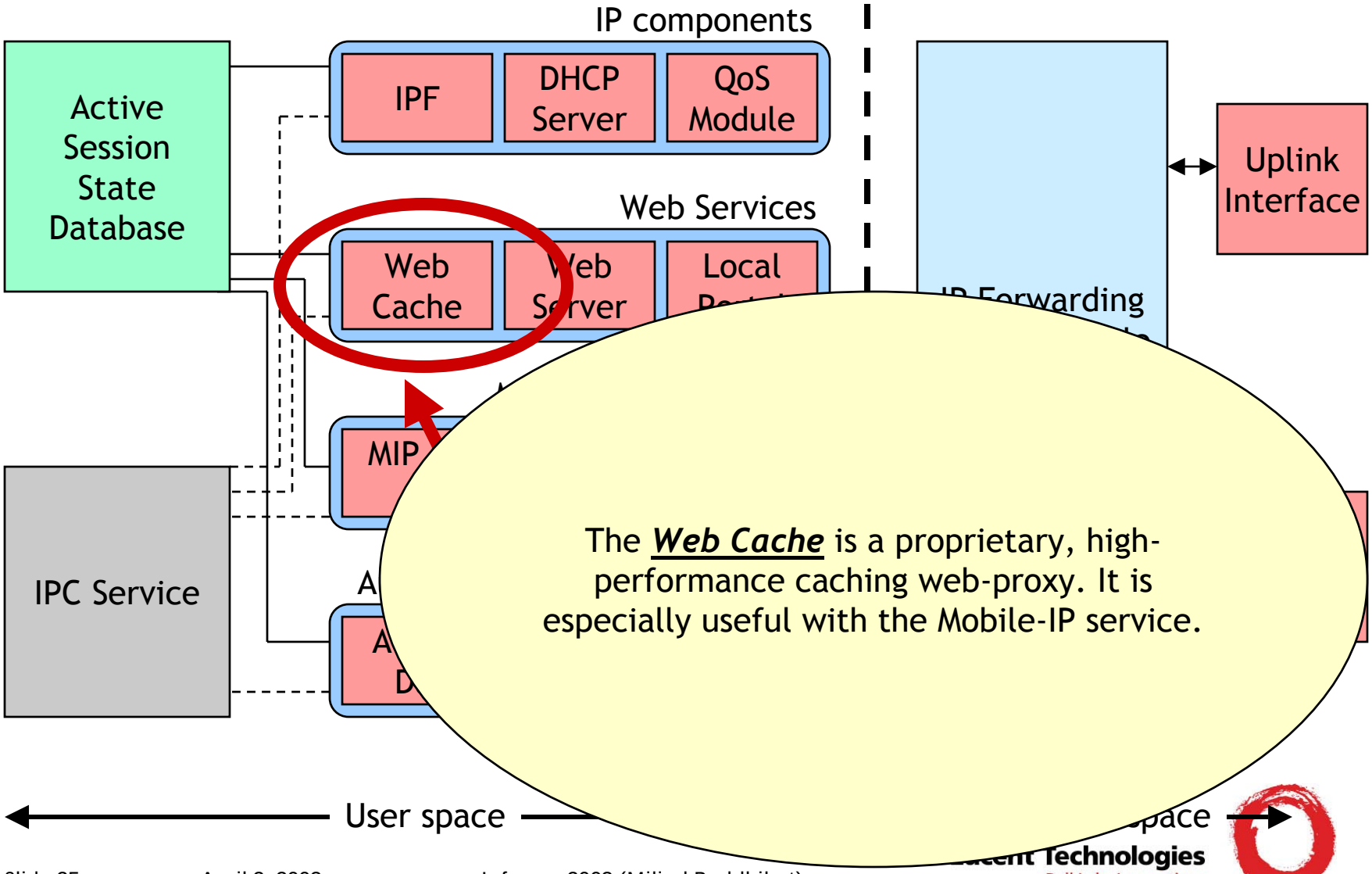


Lucent Technologies
Bell Labs Innovations

QoS for 802.11

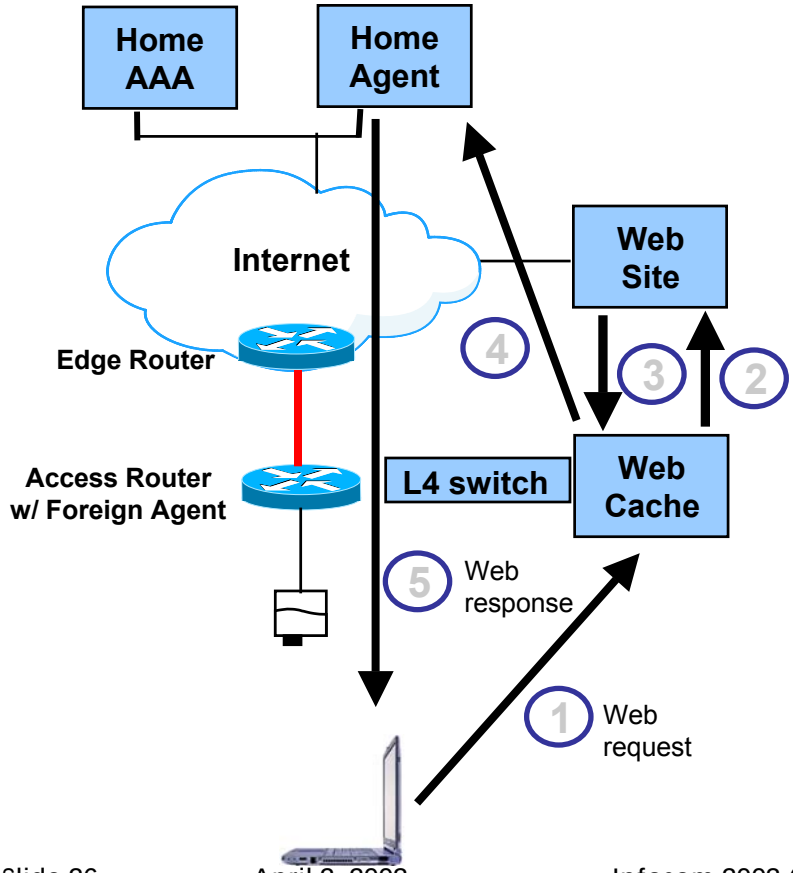
- Per user service level policy obtained from Home AAA database in AAA protocol exchange
  - Three service classes (Gold, Silver, Bronze)
  - Minimum rate guarantees per class (750 Kbps, 500 Kbps, Best-effort)
- Map user population in 802.11 cells to achieve fairness and preserving service level guarantees
  - SNMP queries to 802.11 APs
- DiffServ packet marking and traffic policing
  - Gateway can mark packets even with Mobile IP tunnels
  - Home agent marks packets for 802.11 destined traffic
- Additional enhancements possible with client QoS software

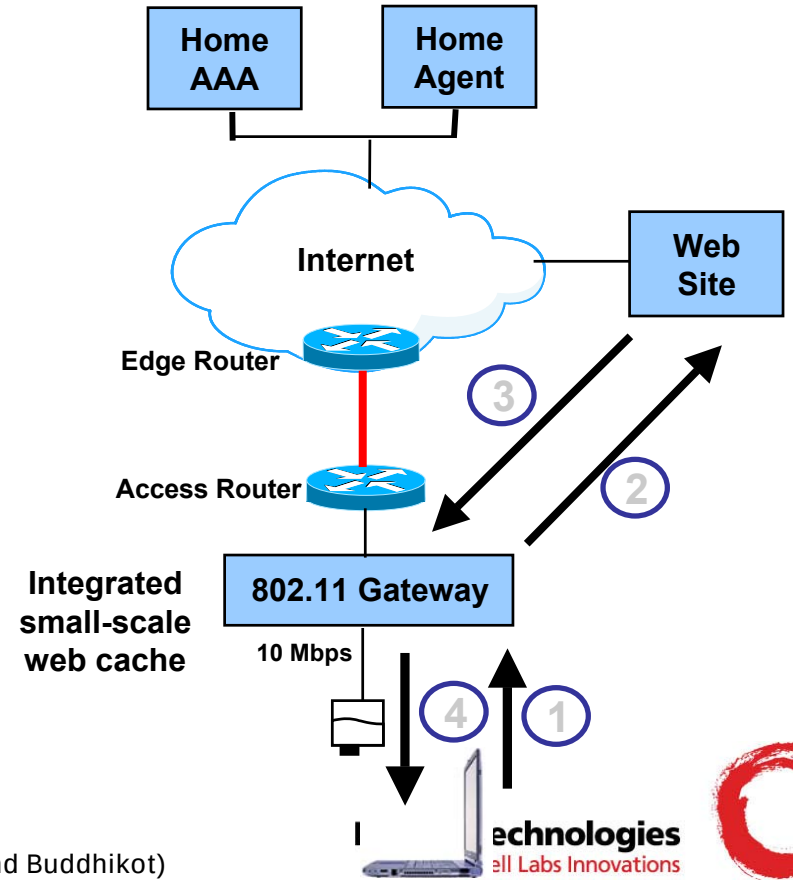
Software architecture of the IOTA gateway



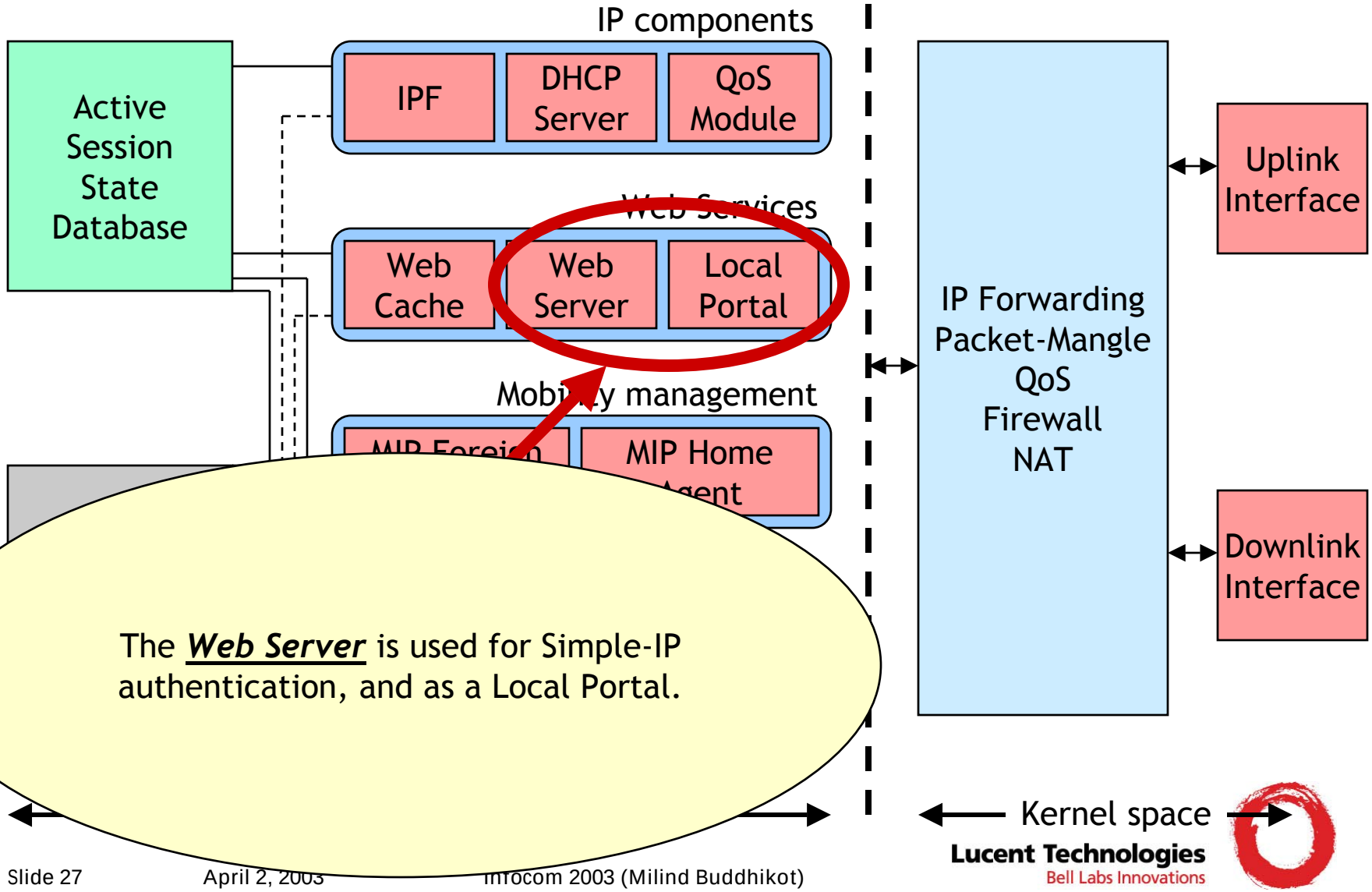
Benefits of Integrated Web Cache

- reduces congestion on access lines to 802.11 network
- provides performance optimization for web traffic by not routing packets back to Mobile IP home agent from cache; can only be done if cache is integrated with foreign agent in same box





Software architecture of the IOTA gateway



The ***Web Server*** is used for Simple-IP authentication, and as a Local Portal.

Software archit

The ***MIP Foreign Agent*** is used to handle Mobile-IP clients. Like the DHCP server, it interfaces with the local RADIUS server to download per-client service, QoS and security policies from the H-AAA, and interfaces with the QoS, IPF and Accounting modules to enforce them.

Active Session State Database

Web Cache

Web Server

Local Portal

Mobility management

MIP Foreign Agent

MIP Home Agent

IPC Service

Authentication and Accounting

Accounting Daemon

RADIUS Server/Proxy

IP Forwarding
Packet-Mangle
QoS
Firewall
NAT

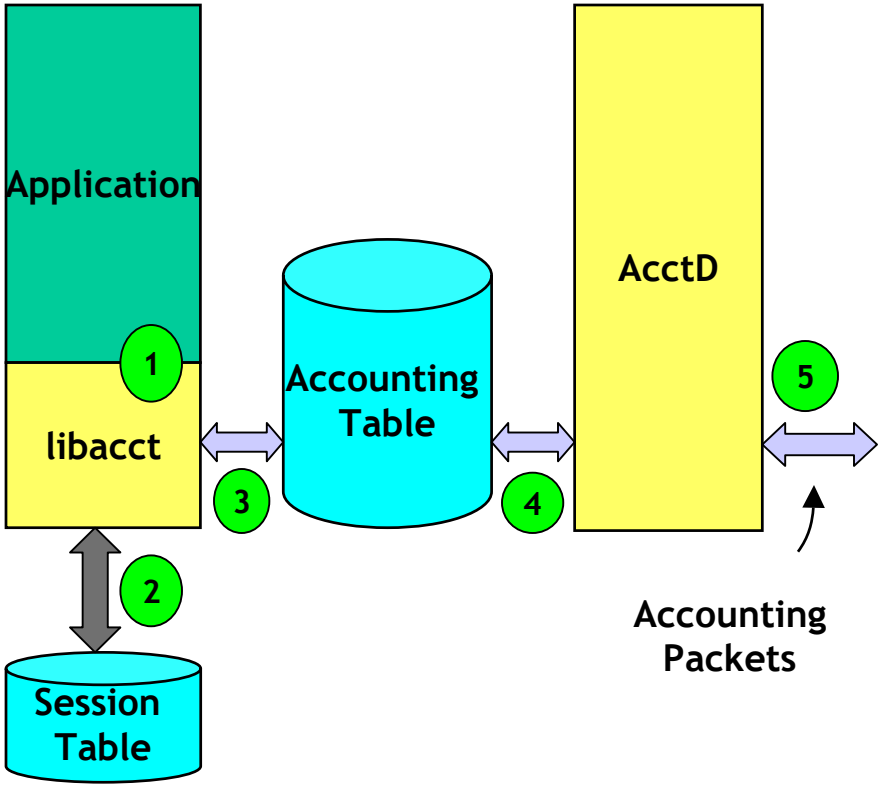
Uplink Interface

Downlink Interface

User space

Kernel space

IOTA Accounting



- Provide accounting mechanism but no pricing policy
- Accounting events generated by applications e.g: DHCP, MIP agent
  - Application compile libacct
- Accounting Start and End events
  - DHCP address allocated (released)
  - MIP registration successful or failed
  - Web authentication succeeds
- **Collect:**start and stop times, duration, packet and octet counts, IP addr etc
- Acctd xfers records to accounting server (e.g.: RADIUS accounting)

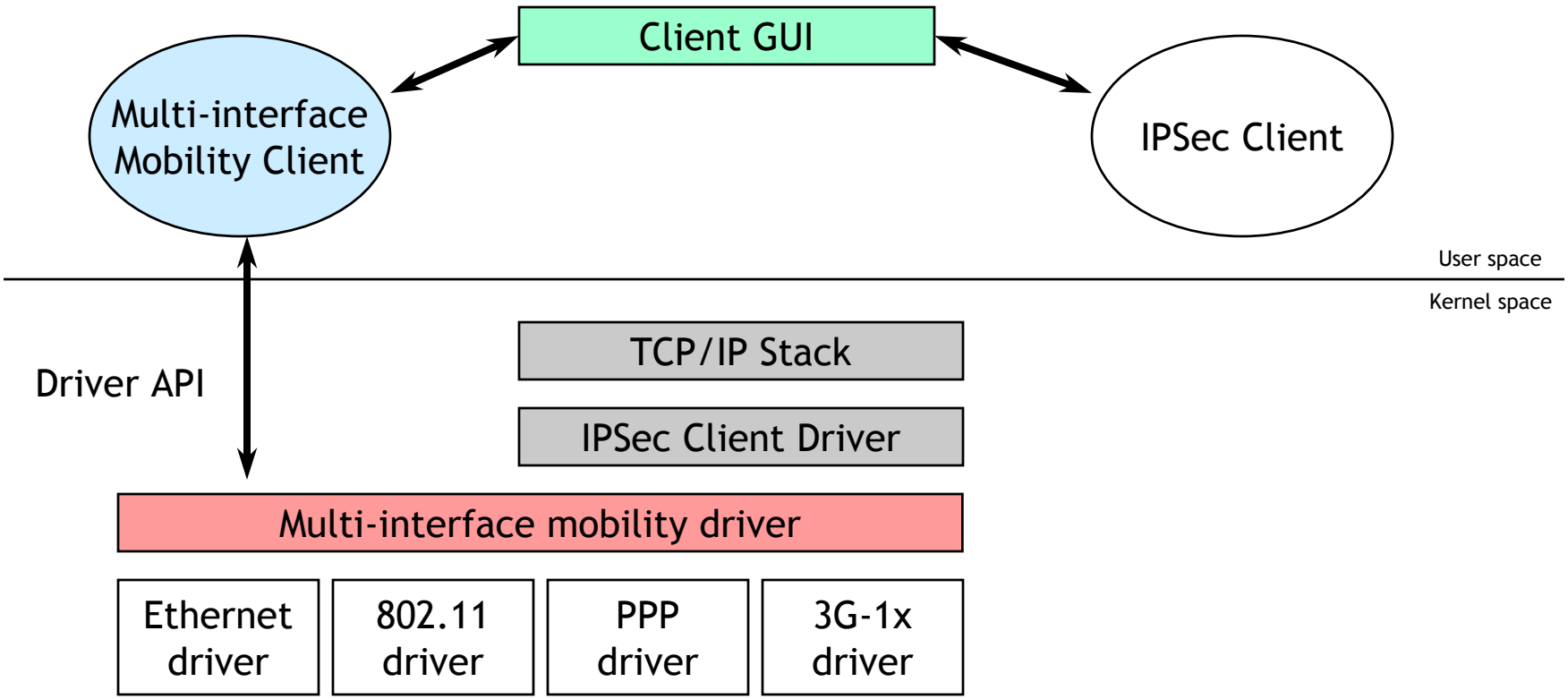
IOTA Client

Lucent Technologies
Bell Labs Innovations

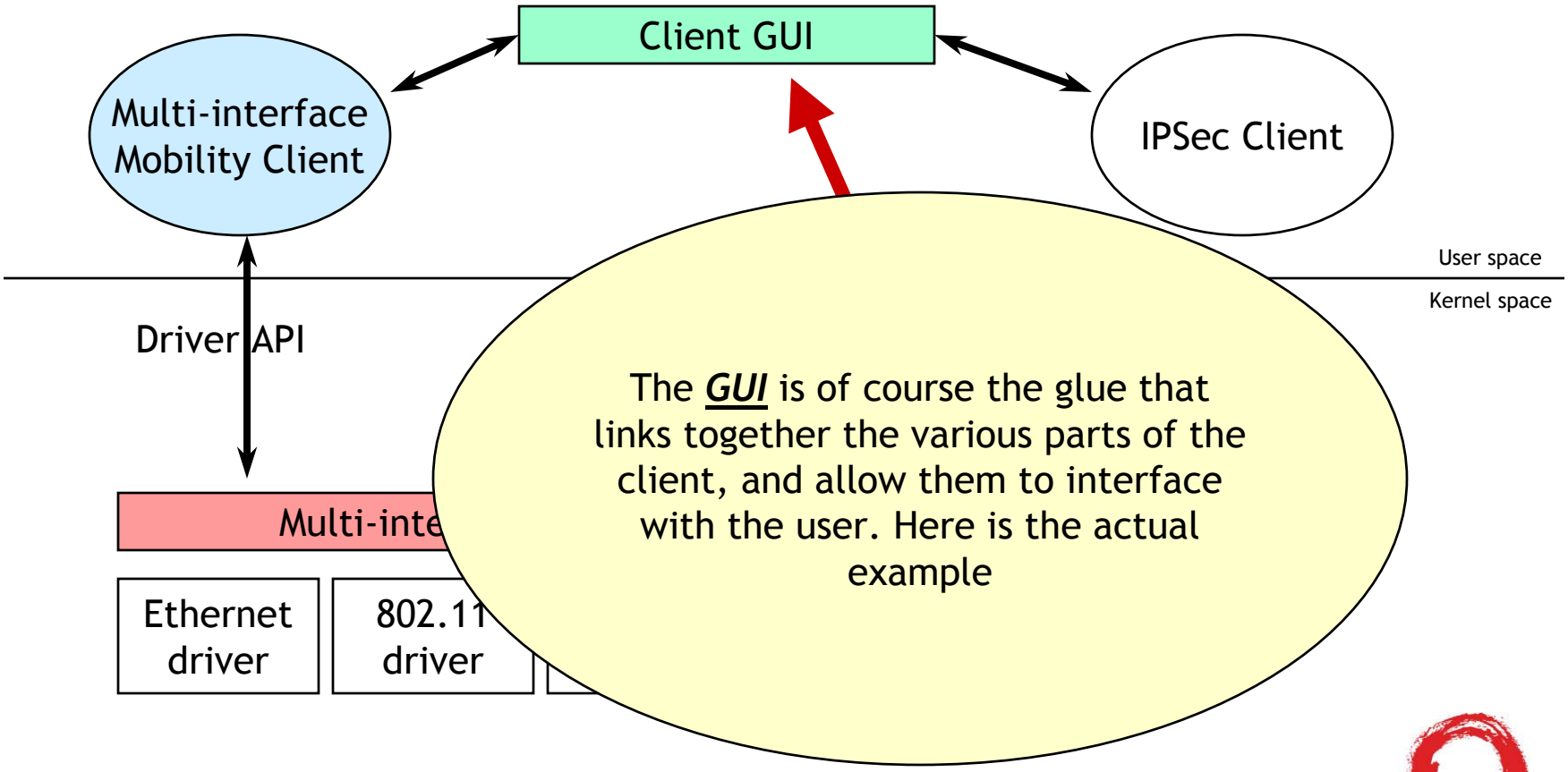
IOTA Client - Features

- Supports mobility across several kinds of physical interfaces
  - List of physical interfaces configured with associated priorities
- Seamless : A user process doesn't see any change in its connections.
- Selection of the interface to use dependent on the user preference, signal strength, availability of a mobility agent in the network.
- Bounce protection algorithm that minimizes the switching
  - between the interfaces,
  - between access points on the same interface
- Allow IPSec tunneling independent of mobility.

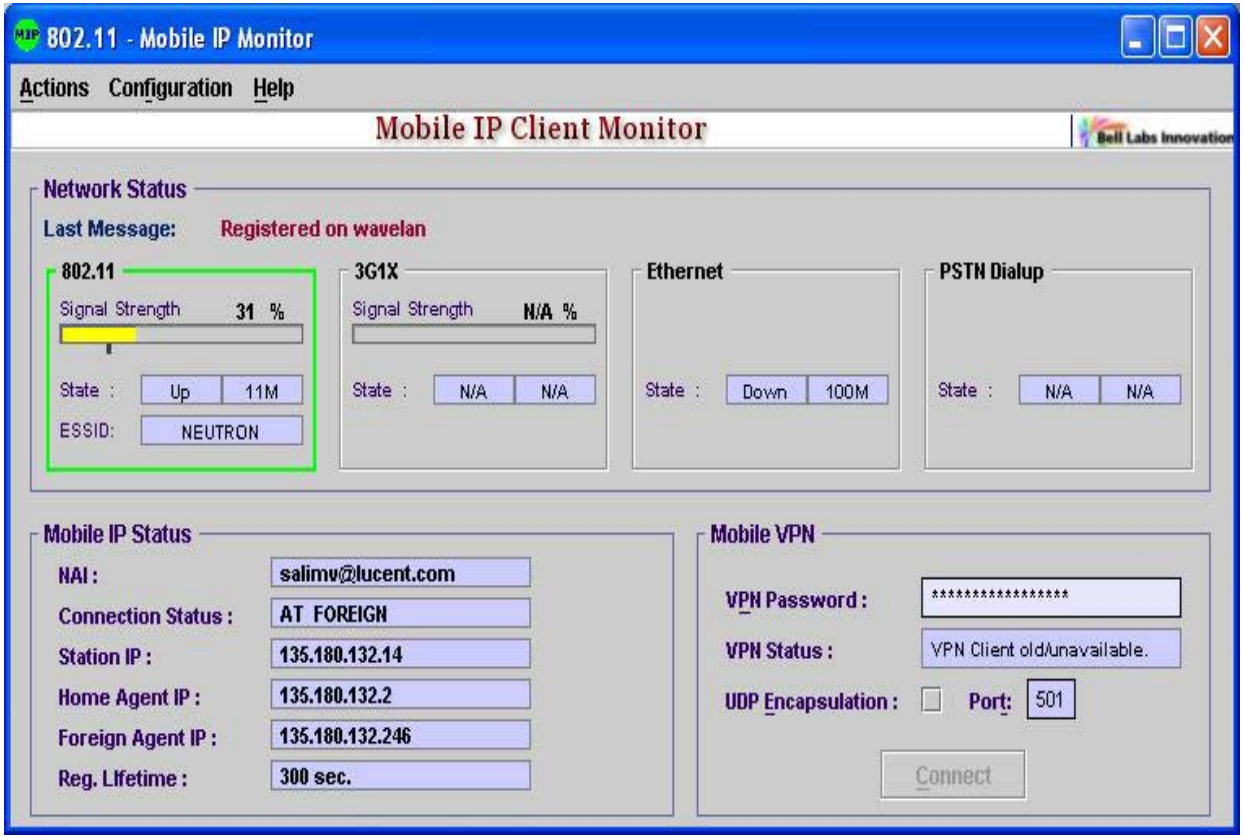
IOTA client architecture



IOTA client architecture

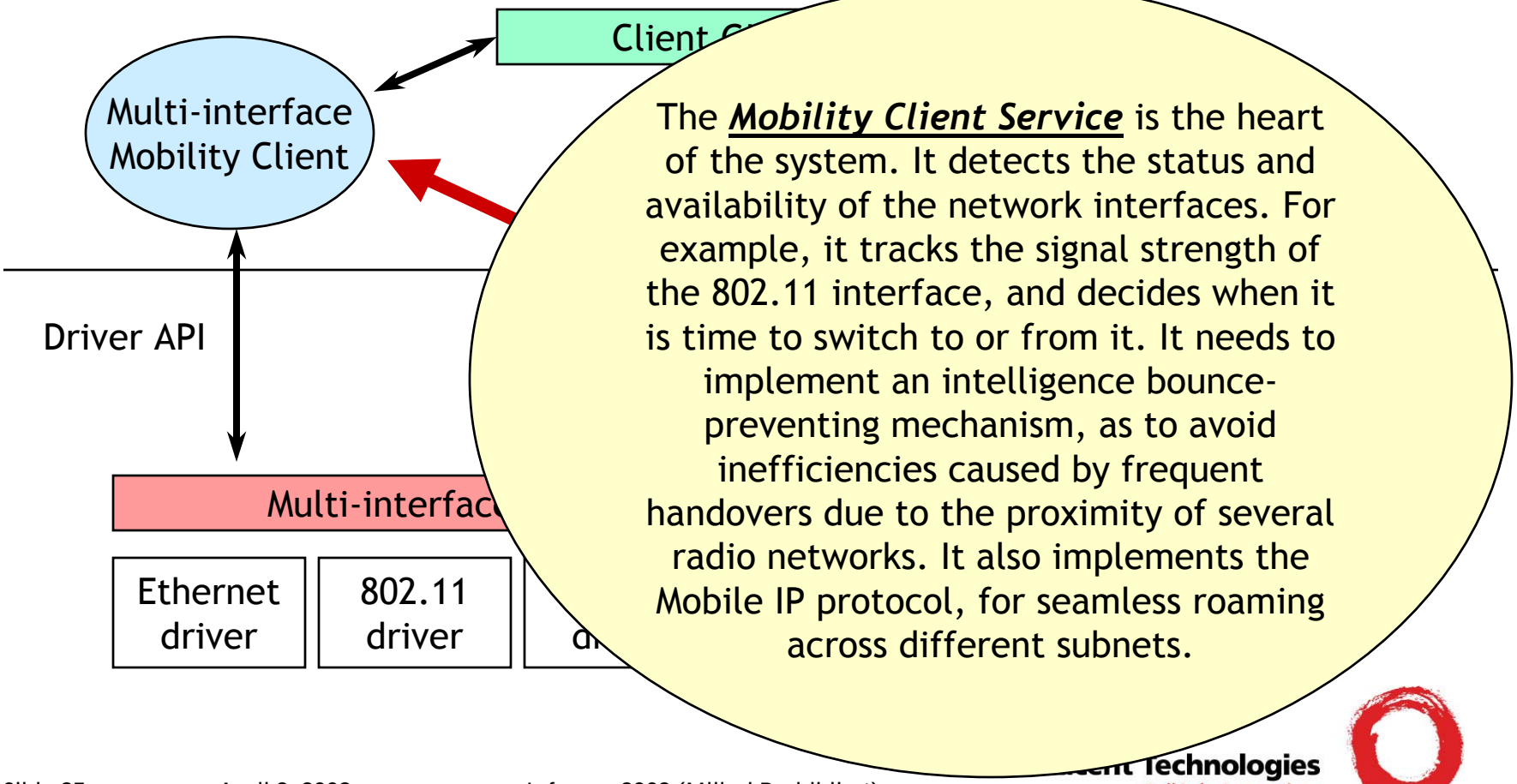


Client GUI



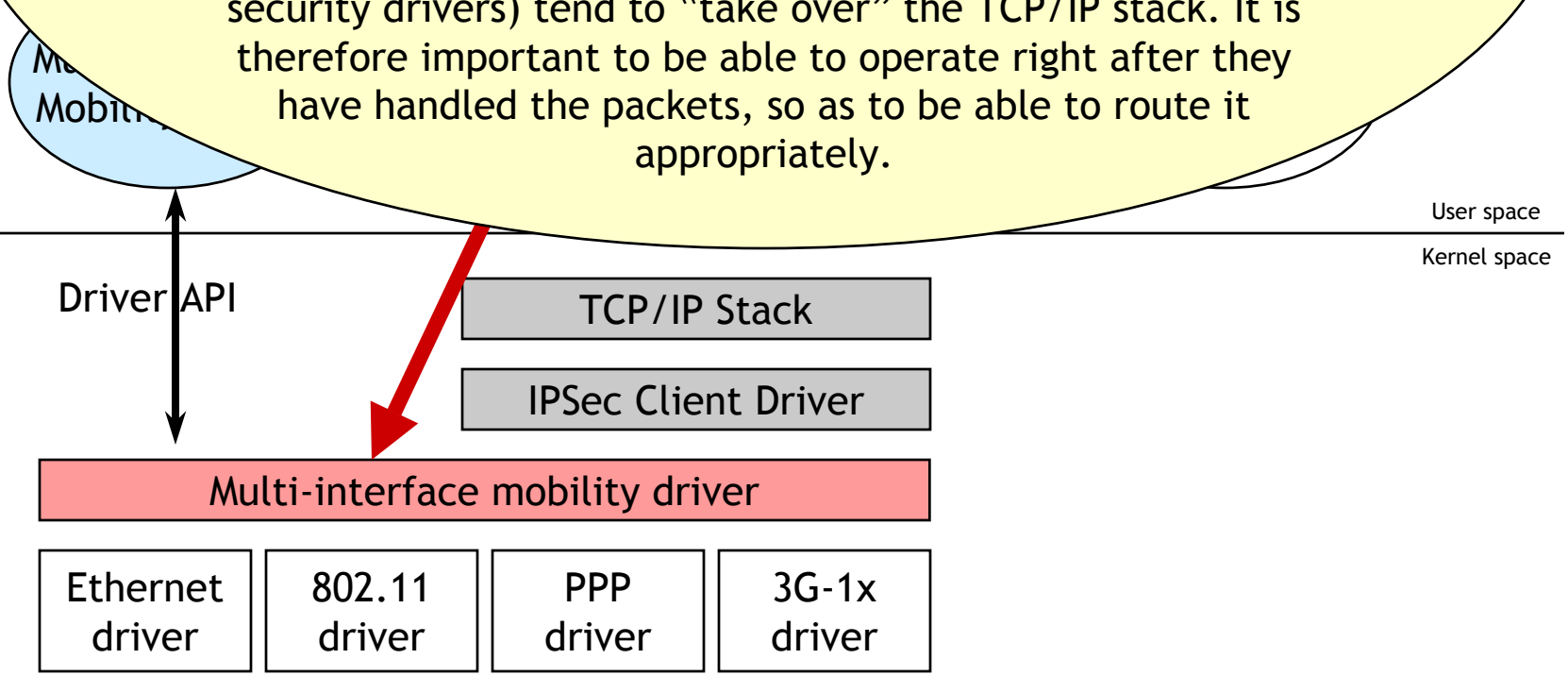
A simple and effective GUI that reports the most current status of the networks and the mobility manager. It also allows users to edit the configuration information.

IOTA client architecture



IOTA cl

The ***Mobility Driver*** handles the IP packets in and out of the system, just before/after they reach the various interfaces. Managed by the Mobility Client Service, it routes the packets to the correct interface. It also handles the decapsulation and encapsulation of the packets when the client operates in Mobile IP co-located FA mode. Note the location of the driver, just below the IPSec driver. This is actually a critical issue, since IPSec (and, in general, security drivers) tend to "take over" the TCP/IP stack. It is therefore important to be able to operate right after they have handled the packets, so as to be able to route it appropriately.



Interface Selection

- Want to elect the best interface
  - Best signal quality
  - Best bandwidth
  - Highest priority (assigned by user)
- Conflicting requirements : often, priority and signal quality
- Impossible to measure precise dynamic bandwidth; we assume priority can be assigned according to the static bandwidth.
- Want to avoid frequent switching between interfaces

Interface Selection (contd.)

- Our design:
  - **Each interface is assigned a priority**
    - Switch to a new interface if it has a higher priority than that of the current one
  - **Signal strength is measured periodically**
    - Switch to a new interface if the new one has signal strength twice that of the current one.
  - **Normalized signal strength is divided into three segments, using two thresholds (high and low)**
    - to avoid bouncing, switch to an interface only when its signal exceeds a threshold, and switch out if signal strength drops a certain threshold.
  - Compute a 'weight' for each interface, based on its signal strength, priority, and if it is the currently chosen interface

Summary

- Opportunity for carriers to strengthen 3G offerings with 802.11 integration
  - using IETF standards (security, accounting, mobility) in 802.11 networks
- 802.11 integration with CDMA 2000, GPRS/UMTS via loosely coupled approach
  - Benefits of simplicity, network efficiency, cost
  - ability to partner with 802.11 Wireless ISPs
- Can be extended to support
  - Location services
  - Network based VPNs

Backup

Lucent Technologies
Bell Labs Innovations

Example Integrated 3G/802.11 Service

- John Doe, has a laptop/handheld with a 3G and an 802.11 interface.
- John Doe likes 802.11 service that many airports offer because of the high bandwidth he could enjoy.
  - 802.11 offers only spot coverage
    - Need to sign-up with many 802.11 providers to receive service in the places he most visits.
  - manually setup and tear-down his wireless connection as he travels from one place to the other.
- John is therefore attracted by the ubiquitous coverage of 3G networks
- John signs with a 3G carrier, which, in turn, has roaming agreements with many 802.11 service providers.

Example Integrated 3G/802.11 Service

- Service provider offers following service options
  - A: $99: Unlimited 3G service (e.g. Verizon Express)
  - B: $125: Unlimited 3G+802.11 roaming
- John selects B.
  - John travels an airport concourse with 802.11 service, his machine transparently switches to the 802.11 access.
- When John leaves the coverage of the 802.11 provider, his machine should seamlessly switch to the 3G access.
- John pays a fixed bill to 3G provider
- 3G provider and 802.11 provider share revenue

Integrating 802.11 and 3G: Service Provider Wish List

- Carrier differentiation
  - Wider data coverage without deploying 802.11 networks
  - Potentially better performance and QoS for data in congested hotspot and indoor areas
  - Better 3G voice
- Subscriber Ownership and growth
  - Offer 802.11 hot spot access to a 3G subscriber as a value add
    - example: €20/month for 3G, €25/month package for 2.5G/3G+802.11 data access on all roaming partner networks
  - Volume subscribers (by millions) for 802.11 operators
- Transparent handoff and roaming
  - Customers with dual radio modem transparently handoff from a 3G to a 802.11 network
  - Roaming agreement between 3G operator and 802.11 operator

Provider Wish List (Goals) contd.

- Use common AAA and billing infrastructure for integrated access
  - Single point for subscribe management and billing
  - Avoid creating duplicate and disparate authentication mechanisms
  - ***Use of one common efficient mechanism***

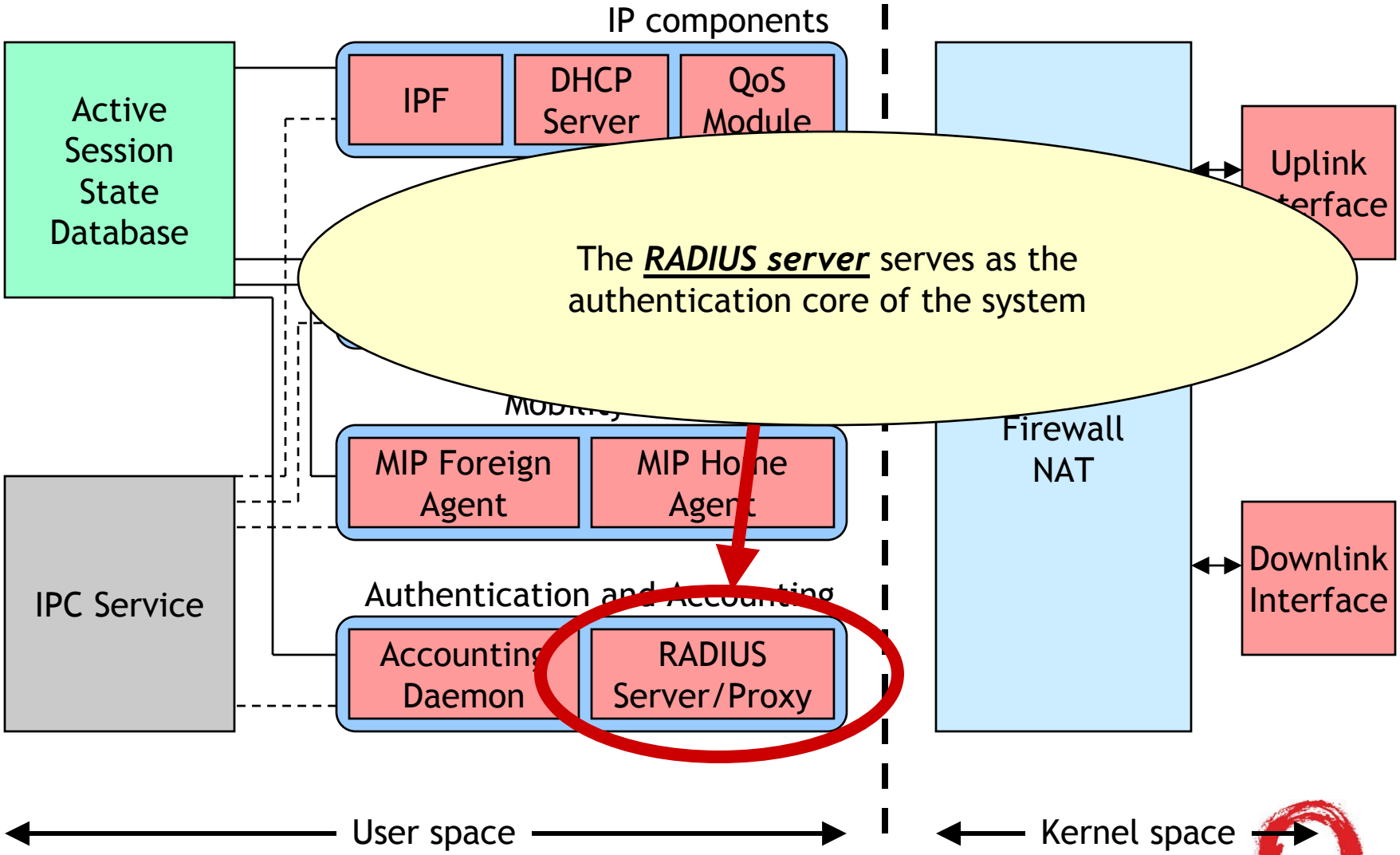
→How to achieve this ?

Provider Wish List (Goals) contd.

- Use common AAA and billing infrastructure for integrated access
  - Single point for subscribe management and billing
  - Avoid creating duplicate and disparate authentication mechanisms
  - ***Use of one common efficient mechanism***

→How to achieve this ?

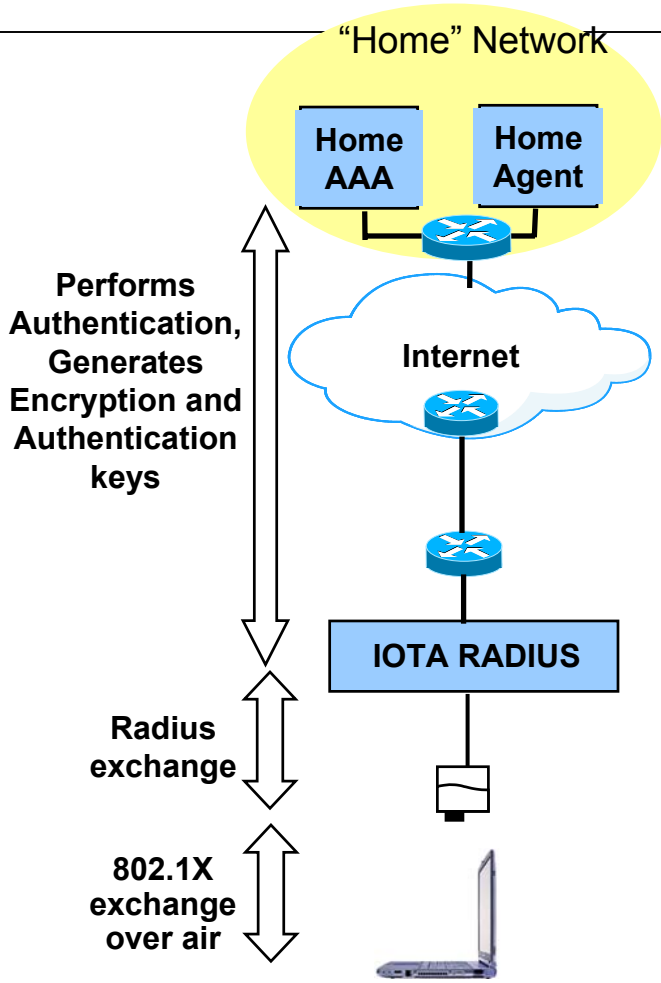
Software architecture of the IOTA gateway



Lucent Technologies
Bell Labs Innovations

IOTA RADIUS

- Used in two modes
  - Local first-tier proxy
  - Standalone local AAA server
- In proxy mode:
  - RADIUS exchanges of auth traffic on behalf of (MIP FA, DHCP, Web server, etc.) with clients' home AAA servers.
- Download per-client policies such as the QoS level to which each client is entitled to, etc.



Algorithm to construct encryption key from passed Master Key

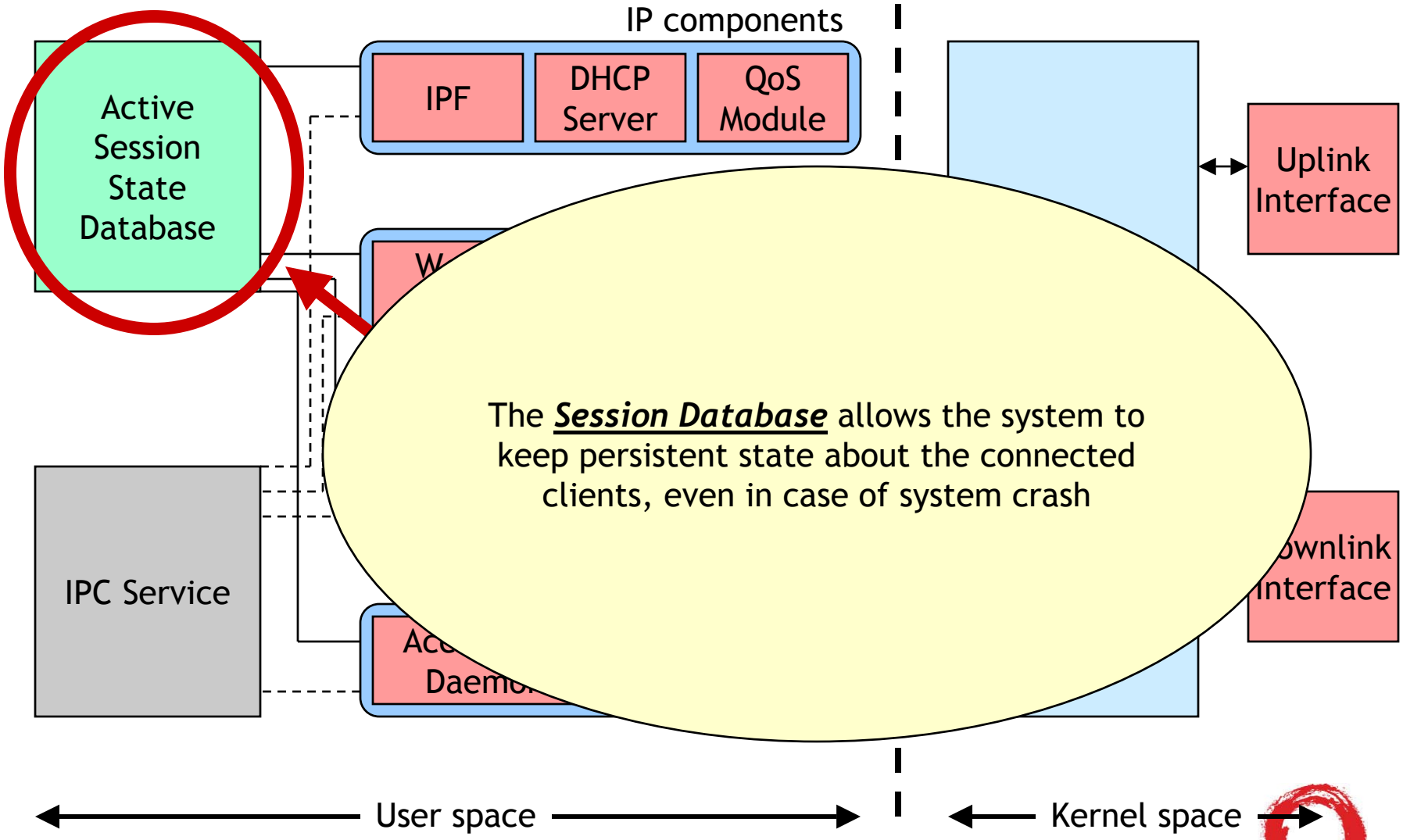
Portable Simple IP Solution

- **First phase:** Common Billing & Authentication support
  - No roaming support and cross network handoff
    - Defined as Simple IP in CDMA2000 standards
    - Common AAA support for 802.11 & CDMA2000
    - Use same authentication credentials on both networks

Seamless Mobility solution

- **Second phase:**
  - Maintain data session across networks and service providers
  - Adds full MobileIP support and cross network handoff
- Since CDMA2000 uses MobileIP, obvious solution is to support MobileIP functions in the 802.11 gateway

Software architecture of the IOTA gateway

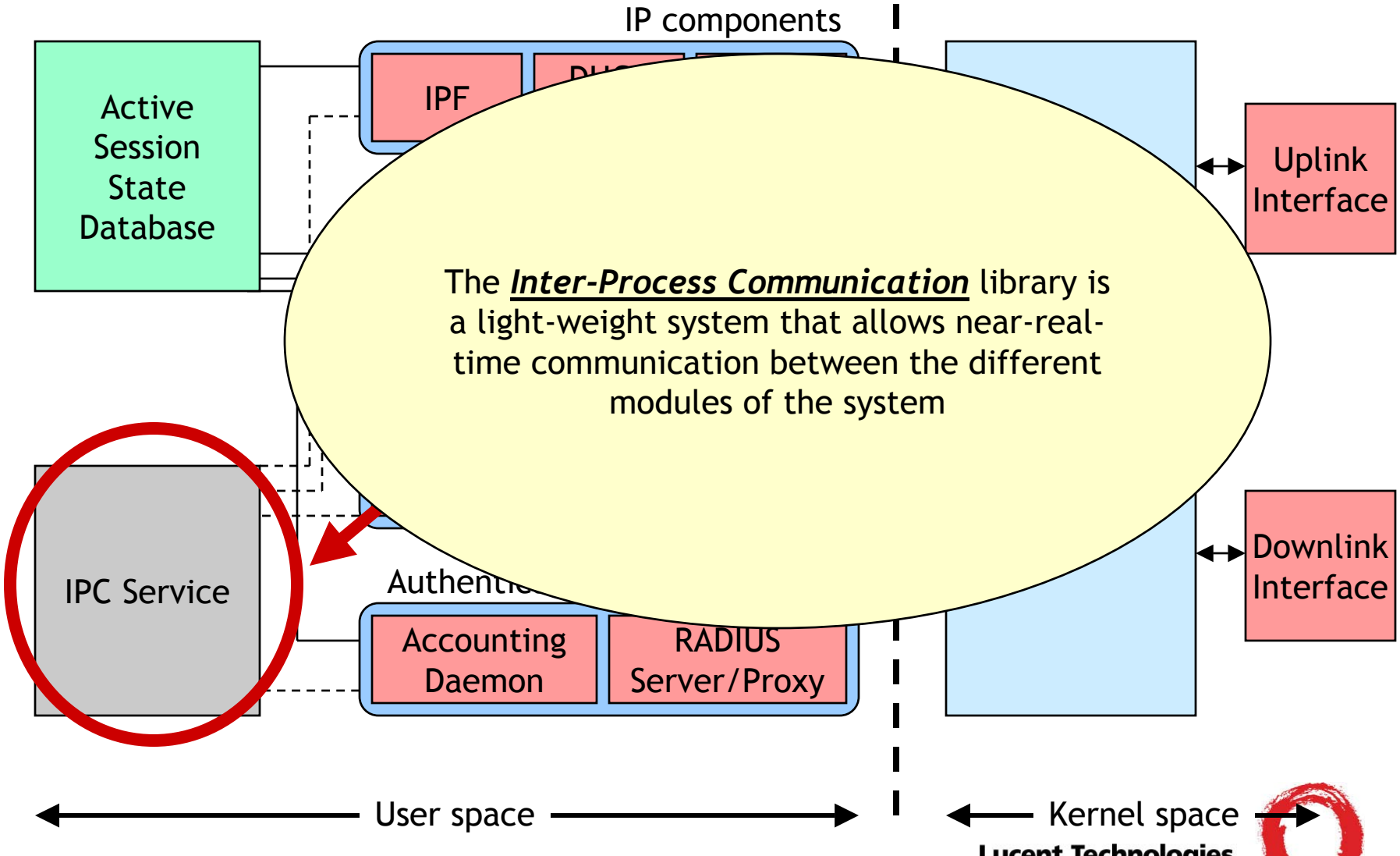


Lucent Technologies
Bell Labs Innovations

Session Database

- Implemented as a in-memory SQL database
  - Backed up on the secondary storage (Crash recovery)
- IOTA modules refer to session state in the database
  - **Session states:** *UnAuthenticated, Authenticated-TrafficBlocked, Authenticated-Traffic-Passed*
  - Accounting records
  - **Session profile:** Traffic class, Minimum Rate Guarantees, preferred authentication method, NAI, SimpleIP/MobileIP mode, Home Address etc.

Software architecture of the IOTA gateway

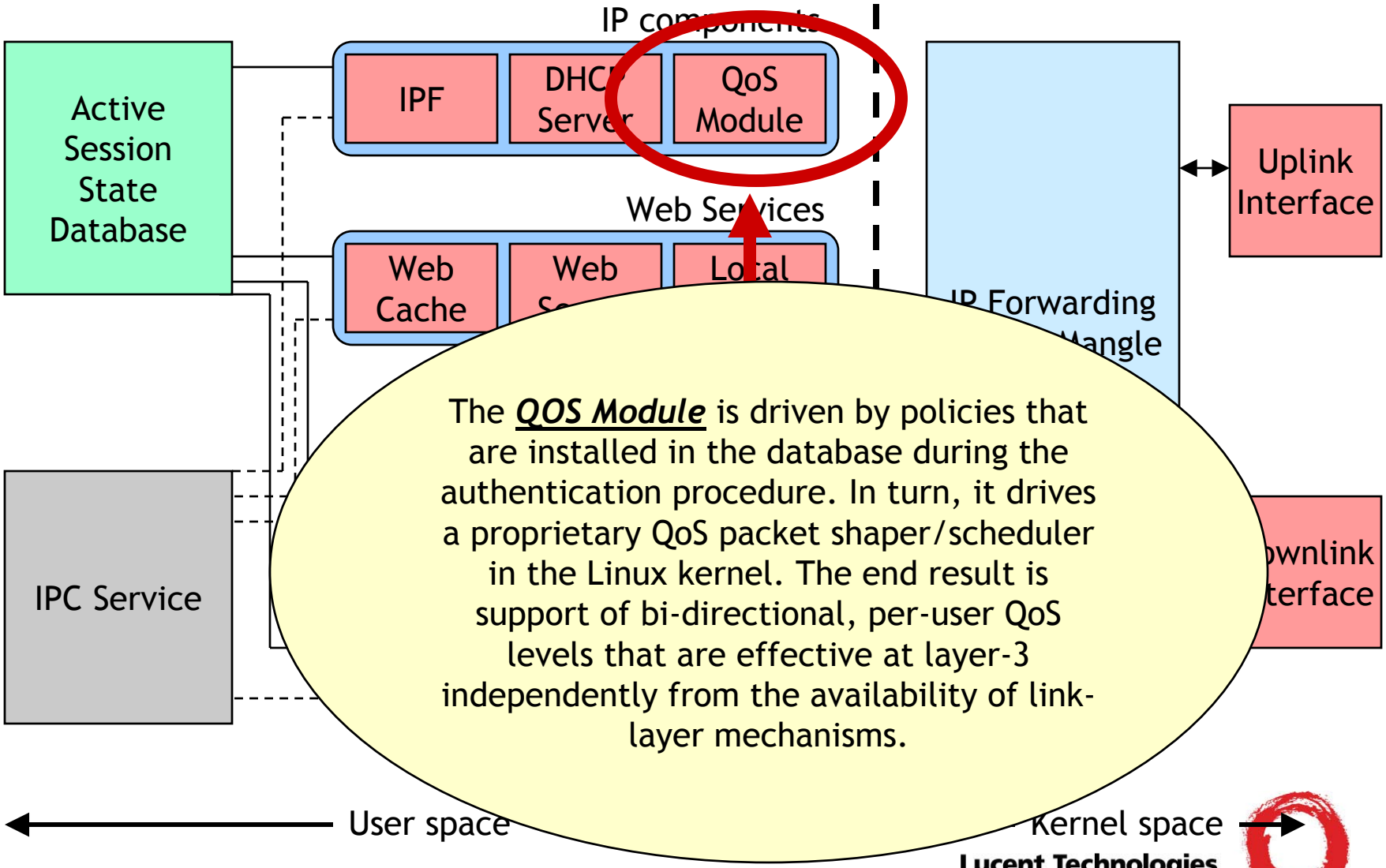


Lucent Technologies
Bell Labs Innovations

IOTA Client Licensing

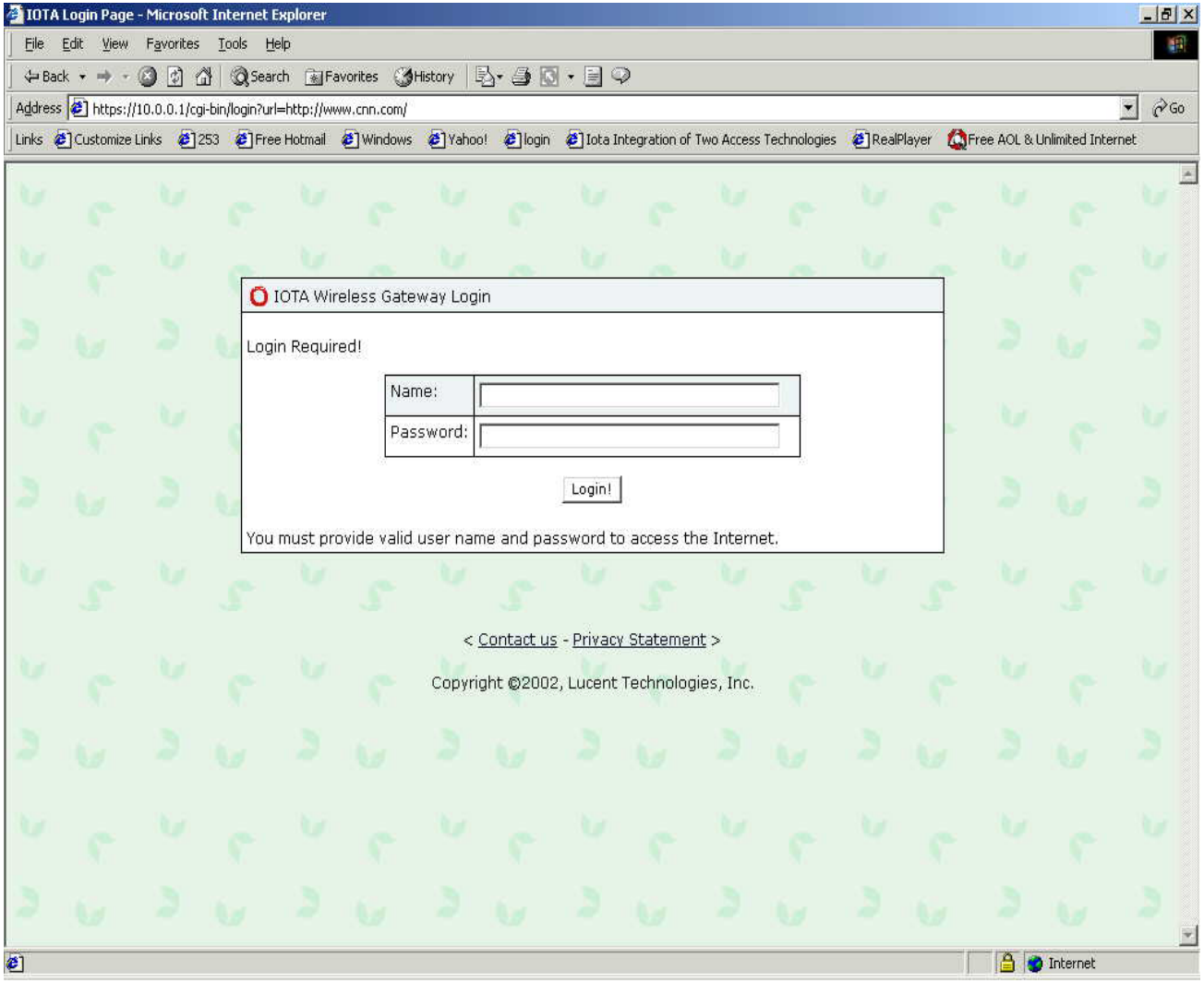
- **IOTA Client Software for multi-interface integration is currently under consideration for licensing with a few vendors**
- It is available for licensing with appropriate agreements
- Please talk to Milind M. Buddhikot (mbuddhikot@dnrc.bell-labs.com)

Software architecture of the IOTA gateway



The ***QOS Module*** is driven by policies that are installed in the database during the authentication procedure. In turn, it drives a proprietary QoS packet shaper/scheduler in the Linux kernel. The end result is support of bi-directional, per-user QoS levels that are effective at layer-3 independently from the availability of link-layer mechanisms.

Web based authentication

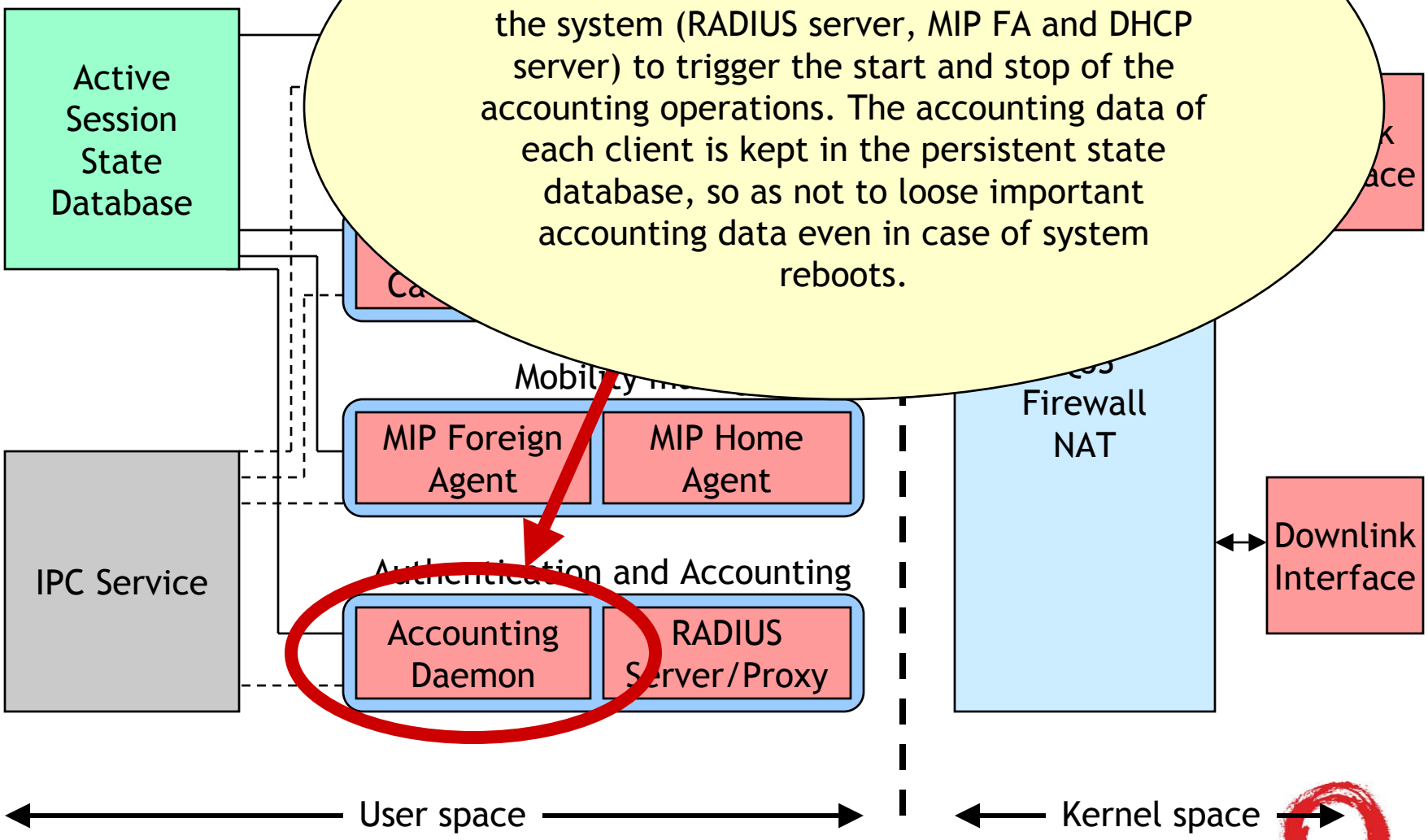


- Password can be One-Time-Password (OTP), SecureID, Biometric Devices
- Traffic blocked until authentication succeeds

Lucent Technologies
Bell Labs Innovations

Software archite teway

The ***Accounting Daemon*** is called by the different authentication and access entities of the system (RADIUS server, MIP FA and DHCP server) to trigger the start and stop of the accounting operations. The accounting data of each client is kept in the persistent state database, so as not to loose important accounting data even in case of system reboots.



Lucent Technologies
Bell Labs Innovations

Client Design Goals

- Support for multiple kinds of physical interfaces
- Modular enough to be able to add a new kind of physical interface
- Support for mobile IP, to provide seamless mobility
- Support for third party IPSec over mobile IP

Calculation of Signal Strength

- Interface selection is based on the weight calculated from priority and signal strength
- Signal strength is measured periodically
- Each individual sample of signal strength can be fluctuating a lot due to environmental changes (such as people moving about)
- We have a few mechanisms to track a stable signal strength
  - Averaging 'n' samples of signal strength measurements
  - Dropping the zero value between two high non-zero values
  - Calculating the slope of the measured signal strength (based on past two values) and predicting a trend for the next interval