Key Technologies and Architectures for Next Generation Mobile Networks

Krishan K. Sabnani, SVP
Networking Research, Bell Labs

August 27, 2007

The Network Evolution

Yesterday…

- Networks were designed to carry voice traffic
- *Data traffic mostly overlaid on voice networks (using modems)*

Volume of data traffic exceeds voice traffic

…Today…

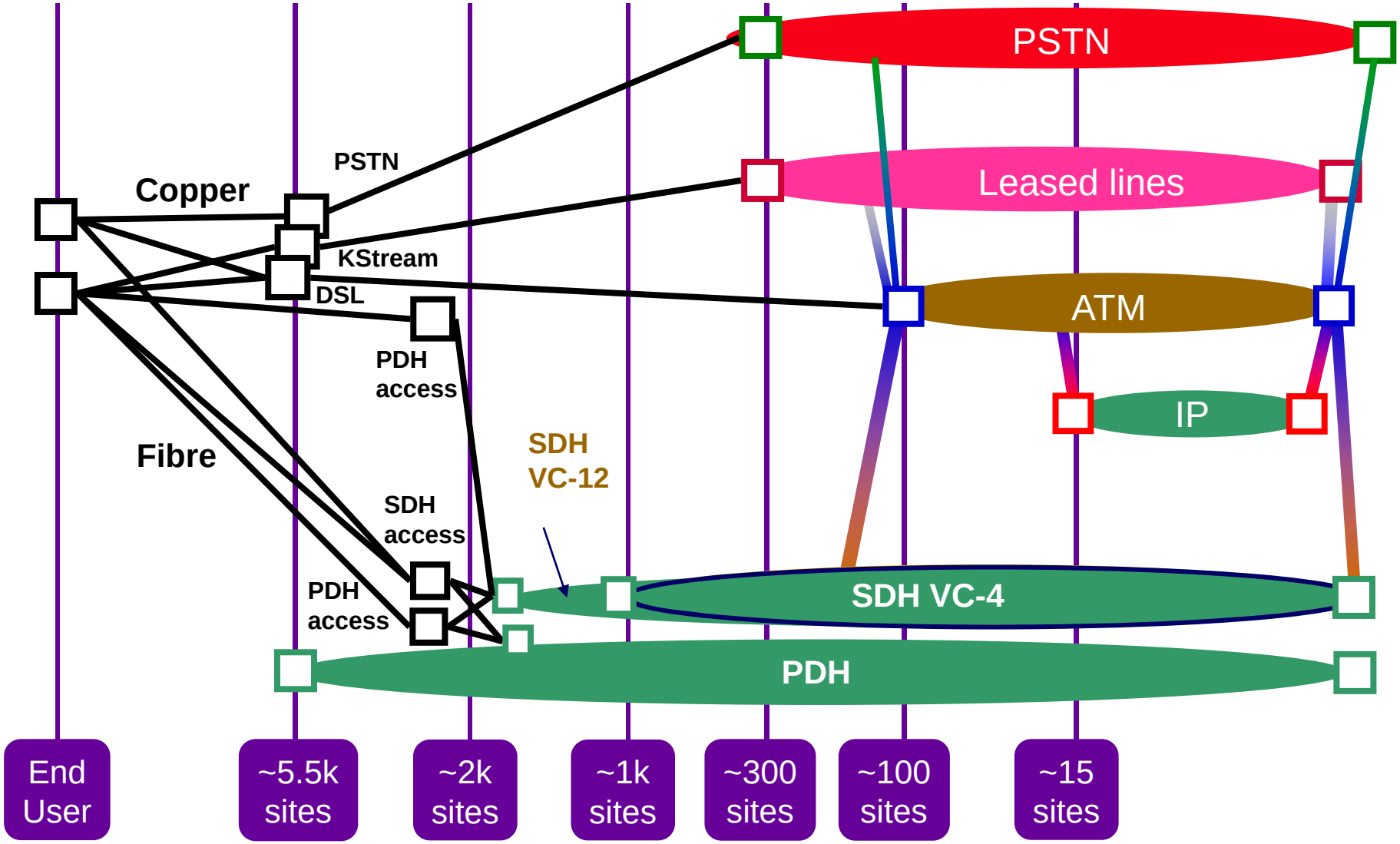
- Networks are designed to carry primarily data traffic
- *Voice traffic overlaid on data networks (e.g. VoIP)*

Content traffic becomes dominant

…Tomorrow…

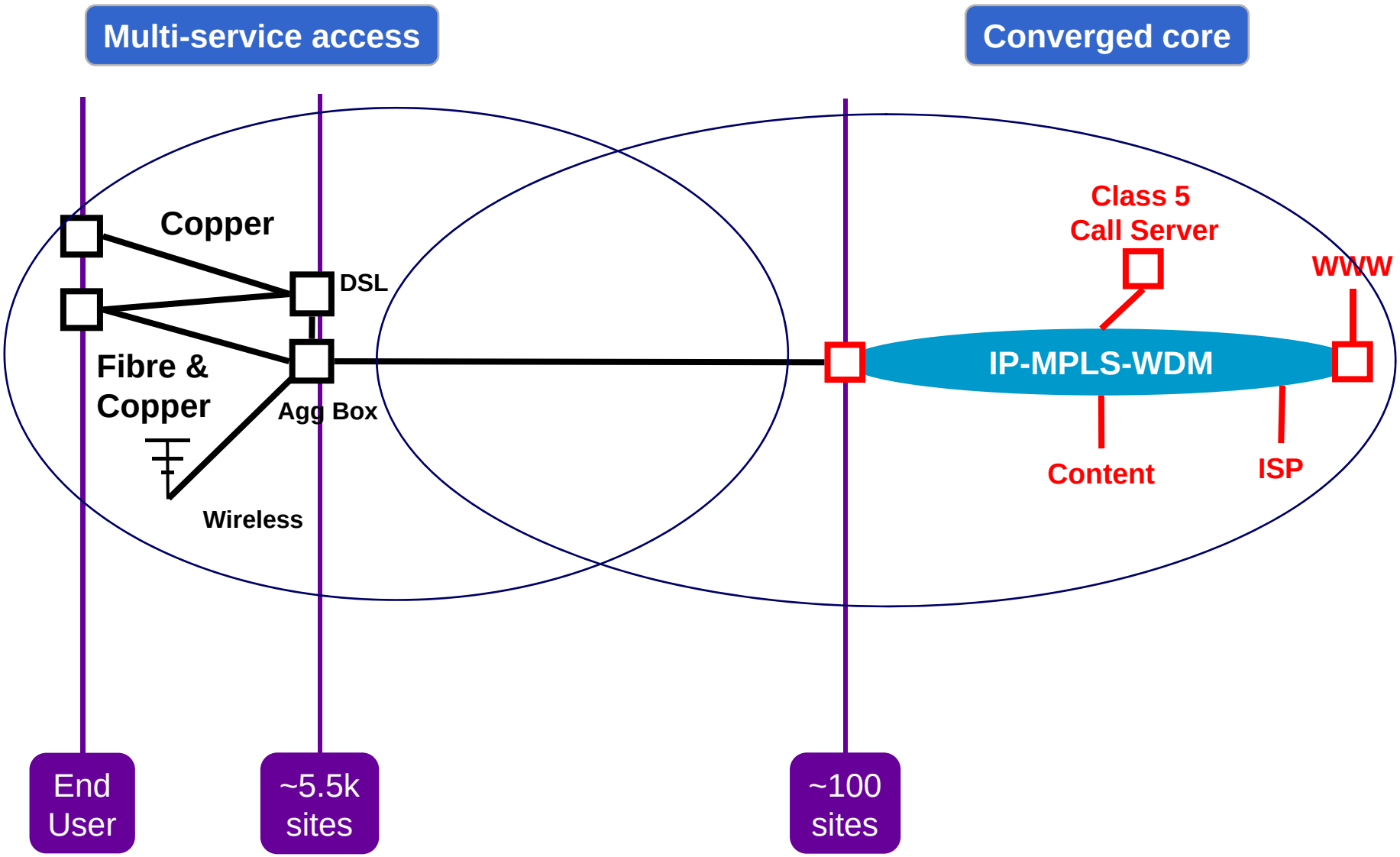
- *Future networks should be designed primarily for efficient content distribution* **and content search/location**
  - **Content distribution should *not* only be overlaid, but built in from ground up**
- **Future networks should also be able to effectively carry best-effort data traffic and QoS-sensitive multimedia traffic**

BT's Current UK Network



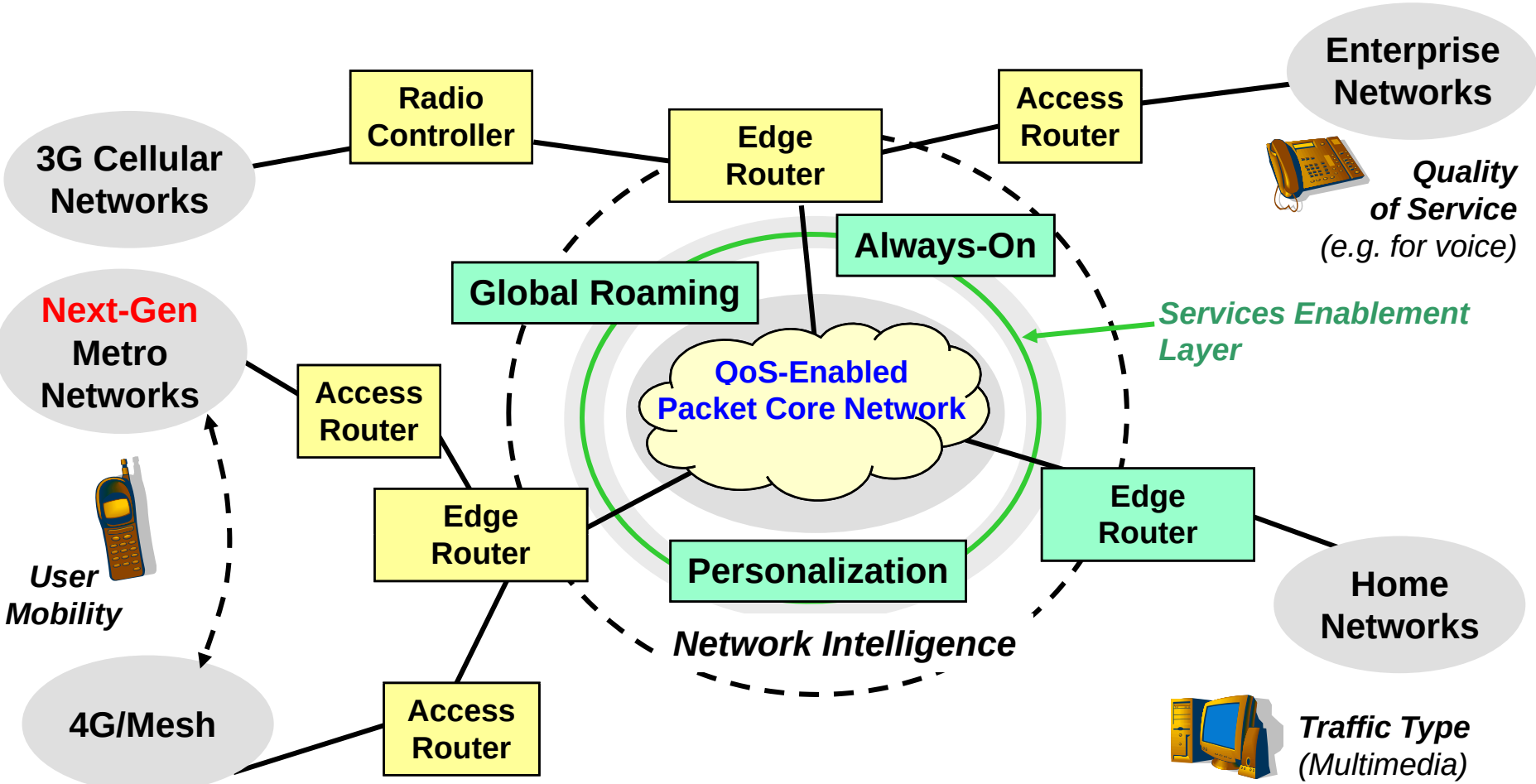
Alcatel·Lucent

BT's Simplified 21CN UK Network



Alcatel·Lucent

Tomorrow's Converged Network



Alcatel·Lucent

Enabling Technologies

- Future Telecom Networks will need secure, quality-enabled, high-speed, and well-managed converged packet cores
- Bell Labs has several breakthrough programs to enable this change. Here are three examples:
  - SoftRouter: A new architecture to deal with increased complexity of data networking
  - Base Station Router: An access router which terminates all radio network processing
  - AWARE System for Wireless DDoS Defense

Enabling Technologies

- Future Telecom Networks will need secure, quality-enabled, high-speed, and well-managed converged packet cores
- Bell Labs has several breakthrough programs to enable this change. Here are three examples:
  - SoftRouter: A new architecture to deal with increased complexity of data networking
  - Base Station Router: An access router which terminates all radio network processing
  - AWARE System for Wireless DDoS Defense

Routers Are Becoming Increasingly Complex

Complexity is an IP "Middle-Age" problem!

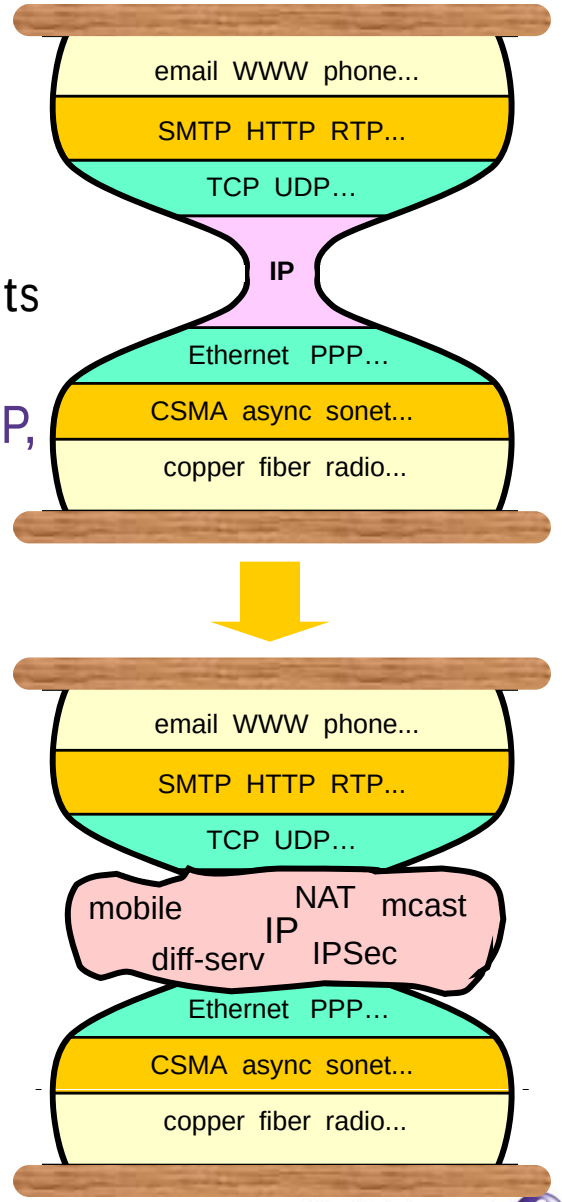
- IP provides end-to-end datagram delivery service to protocols/applications
- IP can use any link-layer technology that delivers packets

Emerging Applications are driving more functions into IP, expanding the "waist" of the IP hour glass

Router vendors incorporate all new IP functions into routers

Complexity is spread throughout the network

- Achieving network-wide objectives such as traffic engineering requires complex translation of global objectives to configuration information in numerous individual routers
- Misconfiguration or uncoordinated configuration can result in poor performance or even *network instability*



Solution: SoftRouter

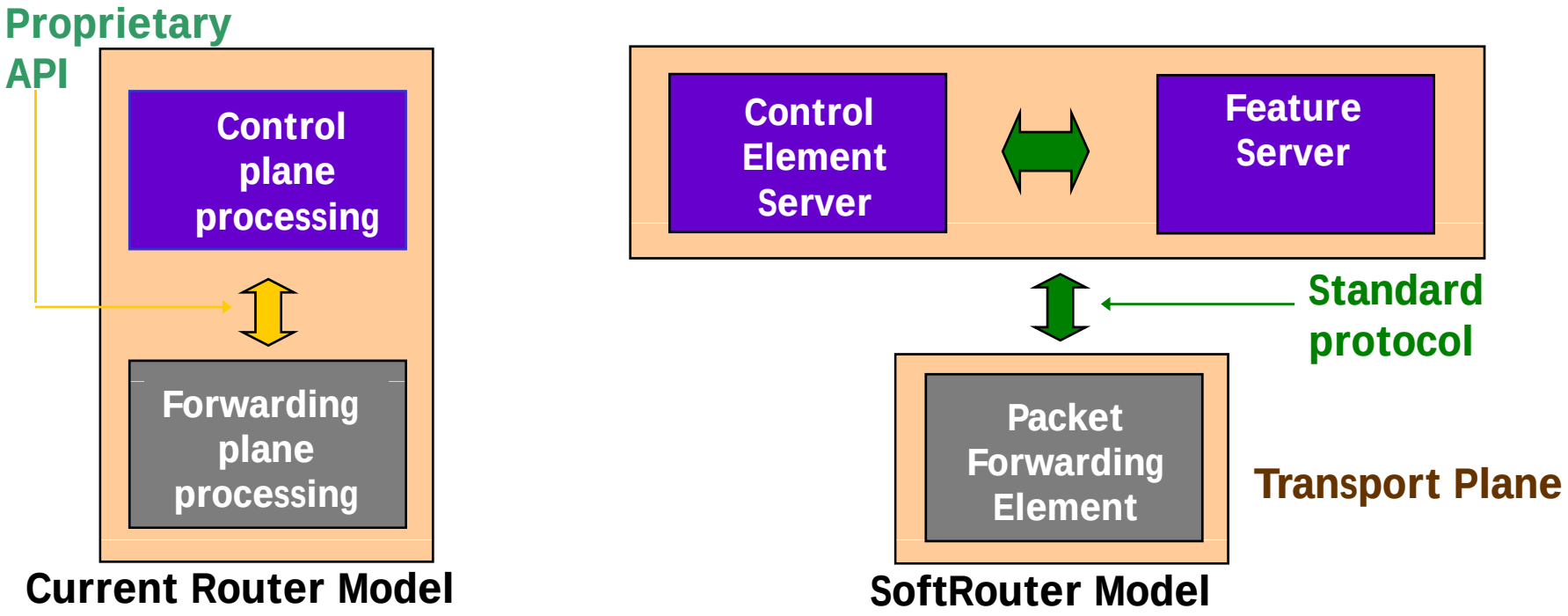
Disaggregation of router hardware from software addresses this problem and has the potential for major additional advantages

Bell Labs has a research program that disaggregates router control and transport planes (called SoftRouter-based approach)

- Transport plane: packet forwarding element
- Control plane: control element server and feature server
- Control element servers and transport plane communicate using standard protocols
- Approach similar to SoftSwitch-based disaggregation of class 5 switches

SoftRouter: New Router Architecture

- **Decoupling:** Separate complex control plane processing from the transport plane
- **Servers:** Implement control plane processing functions on dedicated external control plane servers
- **Standard Interface:** Define standard protocol for control plane servers to interface to the forwarding elements

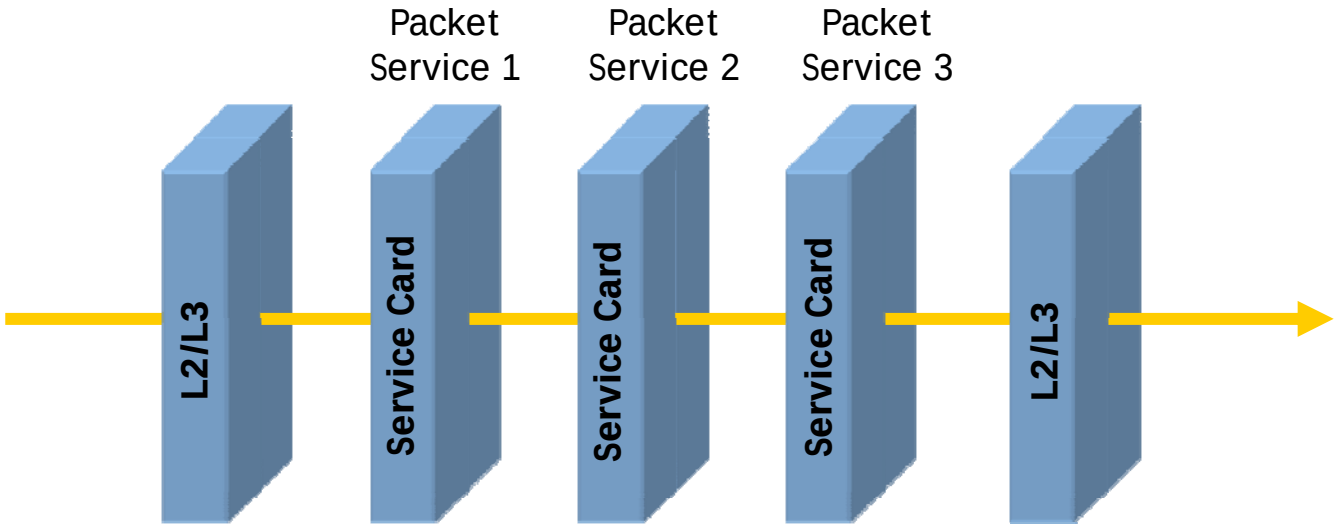


Enabler for Chaining Packet Processing Services

Unix allows processing to be composed via “pipes”

cat infile > prog1 | prog2 | prog3 > outfile

Vision of packet services processing
service cards + service chaining = “network pipes”



Comprehensive Service Management

Reprogrammable service cards + reconfigurable service routing allow flexible composition of edge functions

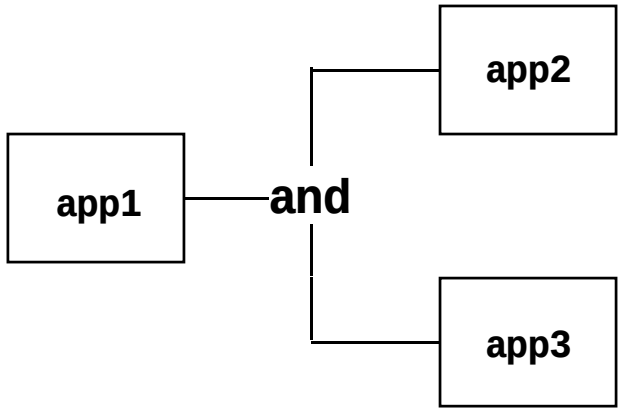
Bell Labs Solution built around service routing

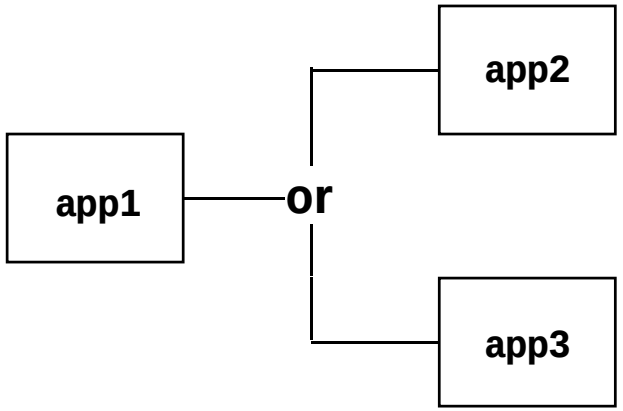
- Allows easy configuration, fault, performance management for edge services
- Configuration: on demand loading of services and definition of service chains
- Fault: active detection and recovery of faulty “services”
- Performance: resource control and statistics on current service performance

Service Chaining Primitives

A service chain specifies an ordered sequence of services to be performed for a packet flow

Abstractly, a service chain is defined by composing individual apps using AND or OR operator



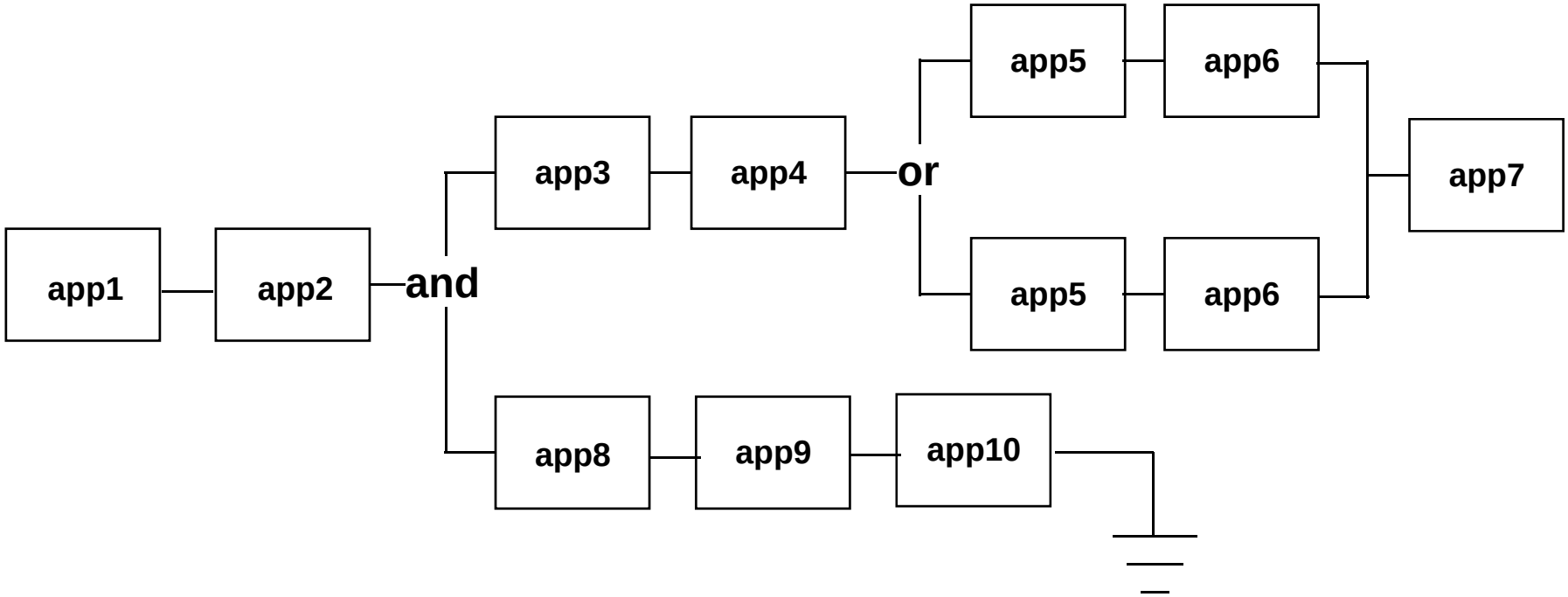


Packets should be duplicated to both app2 and app3 – flow replication

Packets should be sent to either app2 or app3 on a flow basis – load balancing

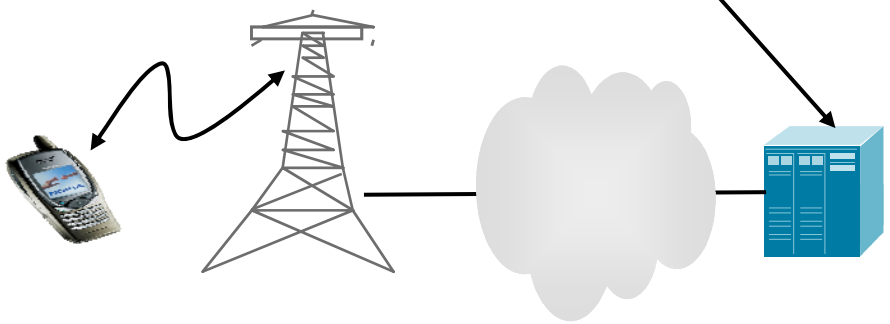
Note: Pt-to-pt case is a degenerate case of either, packet leaving app1 should go to app2

Example Service Chain



Example Application: Integrated Edge Packet Processing

IP Services Platform with programmable services card loaded with packet processing applications



Security: packet filtering/ DDoS protection

Stop attacks to and from mobiles

Control: P2P control/ Bandwidth mgmt

Control services a mobile receives

Application Acceleration/Enhancement: Transcoding/Caching/Voice Quality

Enhance application experience

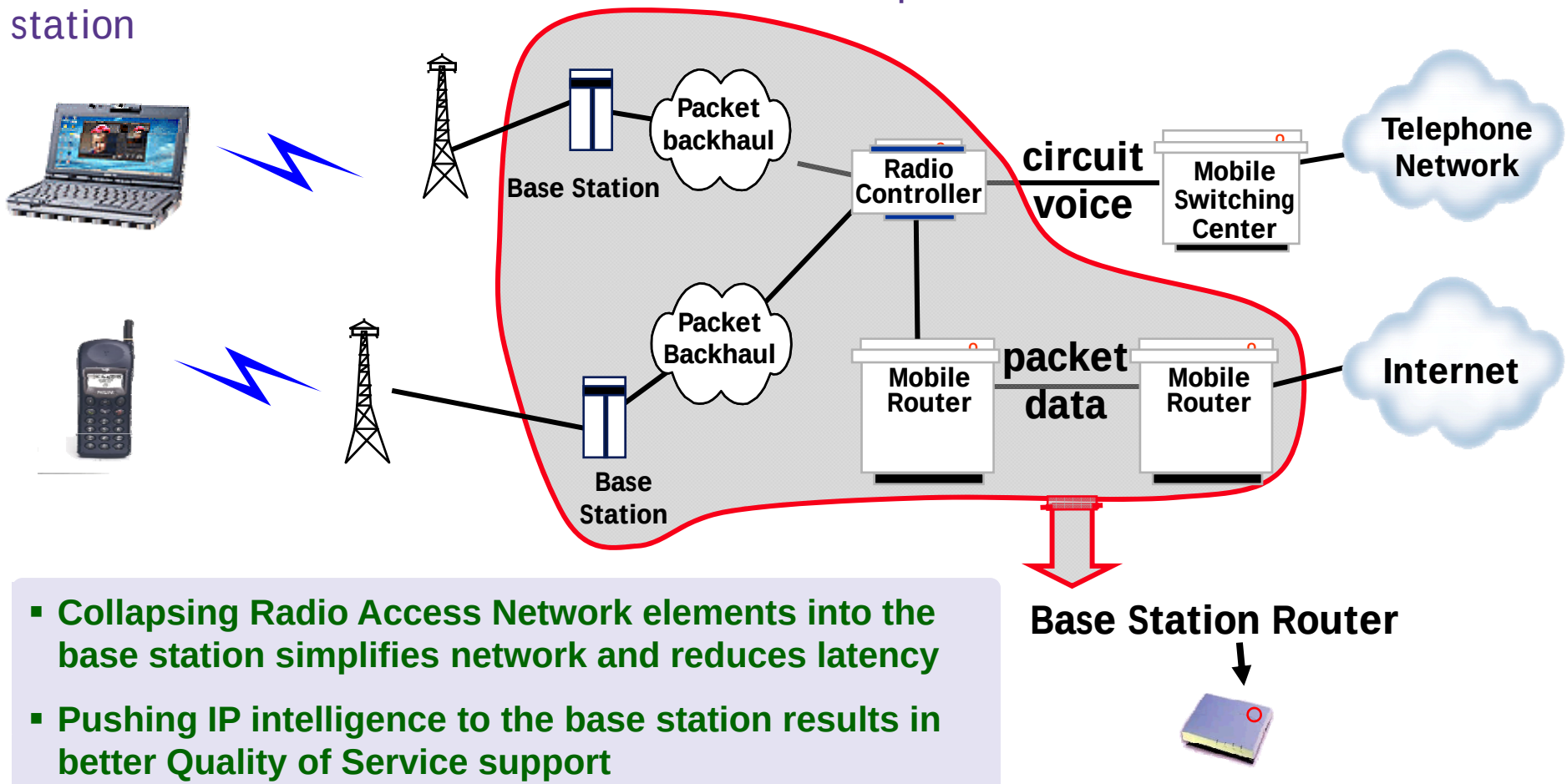
Enabling Technologies

- Future Telecom Networks will need secure, quality-enabled, high-speed, and well-managed converged packet cores
- Bell Labs has several breakthrough programs to enable this change. Here are three examples:
  - SoftRouter: A new architecture to deal with increased complexity of data networking
  - Base Station Router: An access router which terminates all radio network processing
  - AWARE System for Wireless DDoS Defense

Base Station Router: Push Intelligence to the Edge

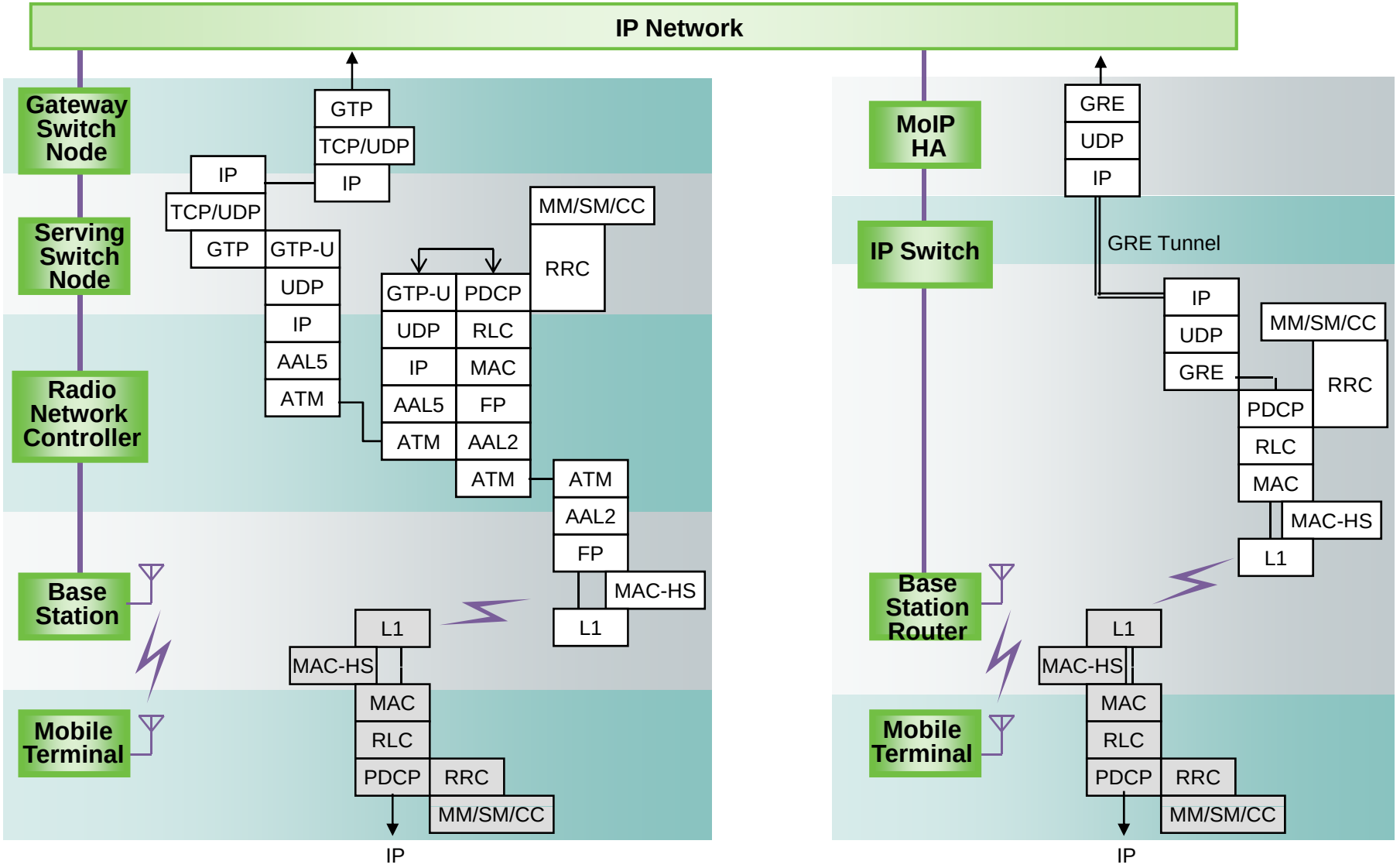
Current wireless networks are complex, involving many network elements, and result in high cost and high latency

Base Station Router terminates all air-interface-specific functions in the base station

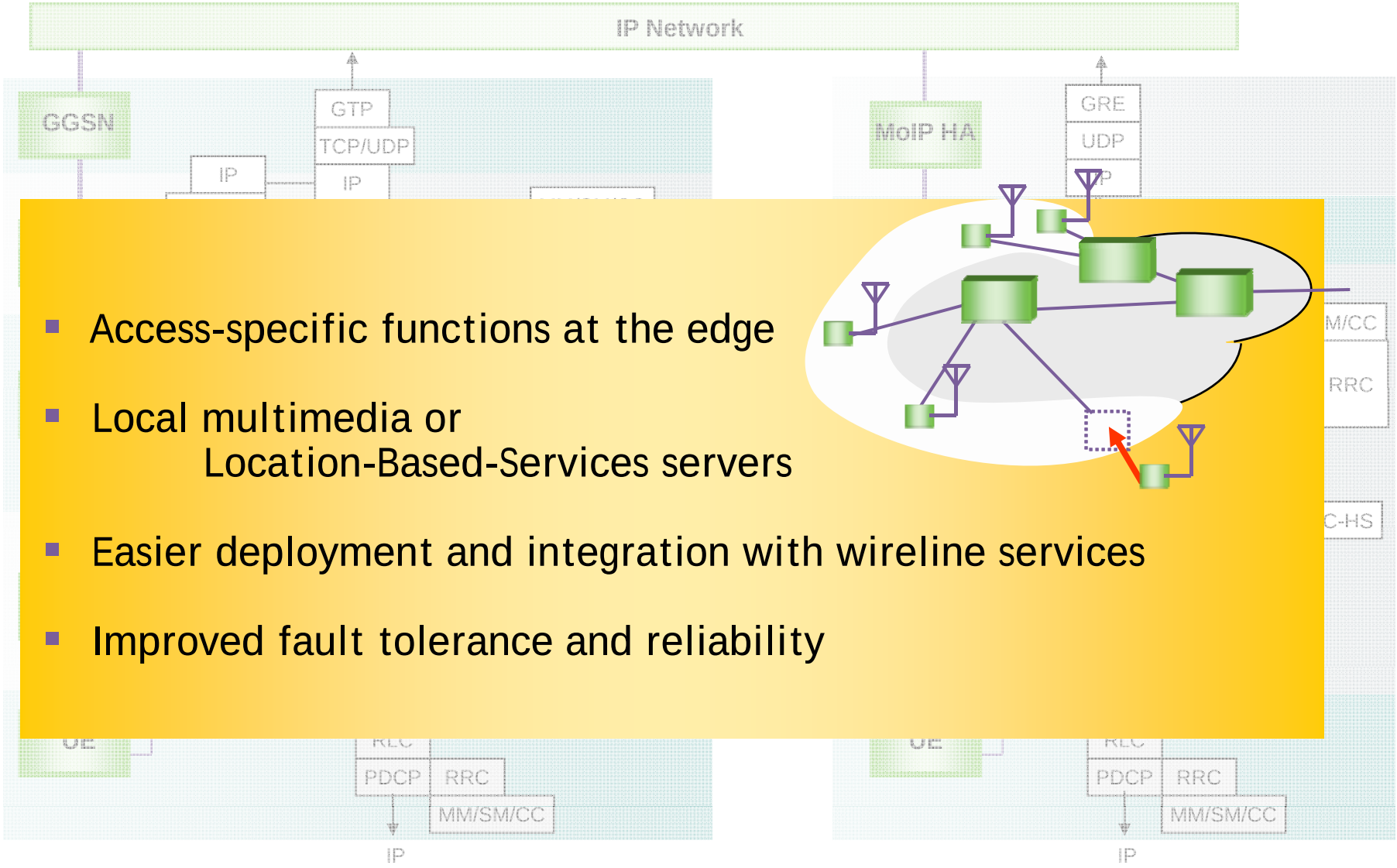


- **Collapsing Radio Access Network elements into the base station simplifies network and reduces latency**
- **Pushing IP intelligence to the base station results in better Quality of Service support**

BSR: Flattening the Network



BSR: Flattening the Network



- Access-specific functions at the edge
- Local multimedia or
  Location-Based-Services servers
- Easier deployment and integration with wireline services
- Improved fault tolerance and reliability

Benefits of Flattening the Network – Driving Simplicity

Lower latency due to flat IP architecture

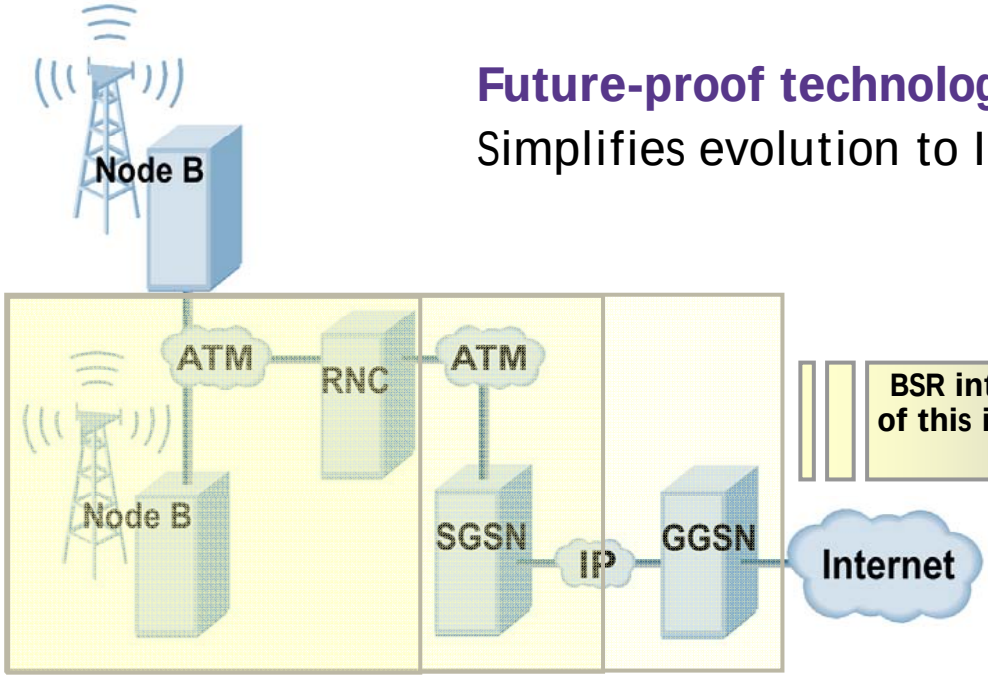
Fewer bottleneck nodes as traffic is offloaded

Capex, Opex optimization

Centralized aspects confined at IP layer for lower scaling cost

Future-proof technology innovation

Simplifies evolution to IMS and LTE



Key Differentiators: Full Plug & Play

Step 0 : Factory

Product identifications are programmed and labeled (bar code and identification)

Step 3 : Plug the Femto

Power-on the Femto
Auto-Configuration procedures starts:
A. Initialization to connect to BSR Gateways
B. Authentication
C. Auto-configuration of initial parameters
D. Check Femto location
E. Registration of authorized terminal

Step 2 : Subscription Confirmed

End user receives confirmation of the subscription and login information
Includes the Femto if he/she had subscribed by web

Step 1 : User's Subscription

The user subscribes to the service (in a shop or on the web)
He/she selects the type of CPE and service set
He/she fill-in his/her personal details

Step 4 : Femto is working !

User receives a confirmation call or SMS on his mobile
Register up to 16 terminals

FemtoBSR System fully integrated in Customer's IT to enable Plug & Play

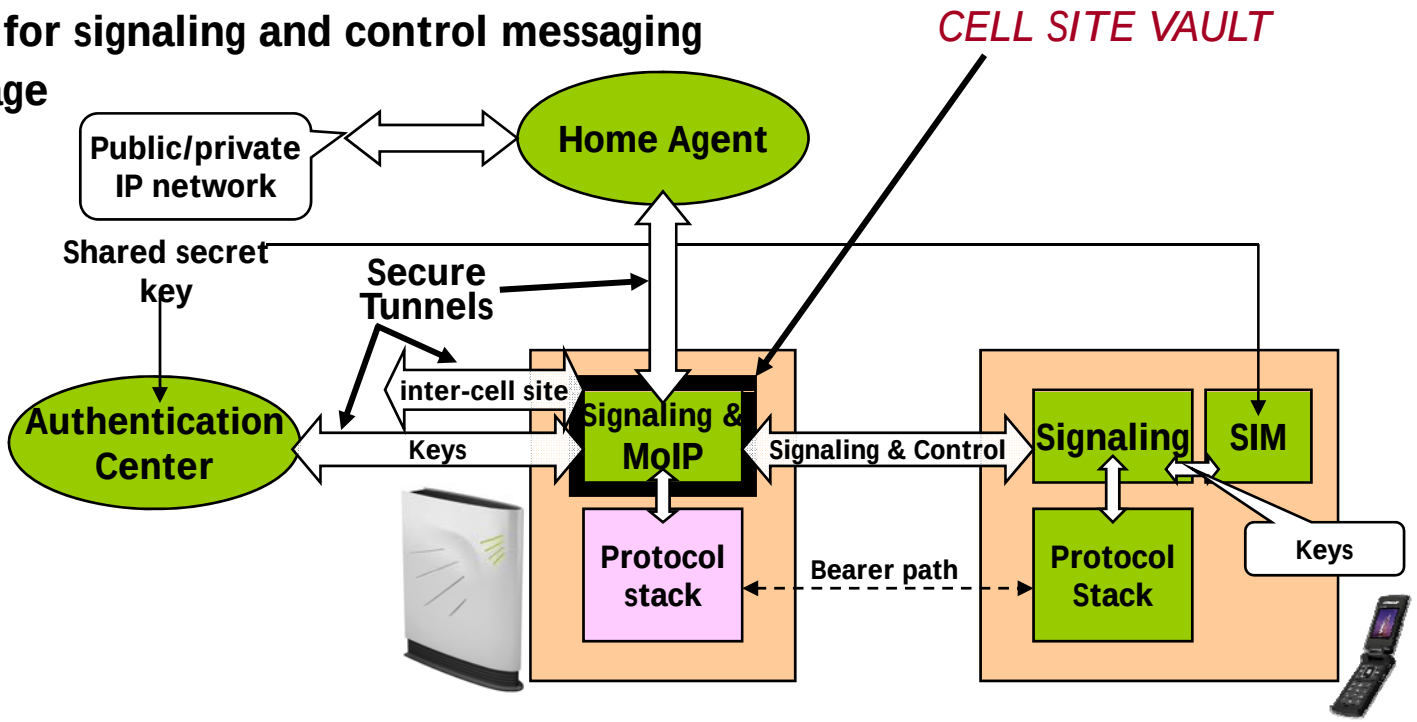
Alcatel·Lucent

Key Differentiators: Security Architecture

Future picocells and femtocells will be deployed in non-secured locations (homes, public locations, etc)

Need a secure environment inside the cell where trust-related functions can be safely executed, eg:

- **Cell and user authentication**
- **Integrity checks for signaling and control messaging**
- **Secure key storage**
- **Data encryption**



The Cellsite Vault is a tamper-resistant, trusted, computing and storage environment within the BSR for where all security-related functions are safely performed

Lucent Technologies' Base Station Router Receives CTIA Emerging Technology Award

Revolutionary Product Takes Top Honors for Most Innovative In-Building Solution

LAS VEGAS – Lucent Technologies (NYSE:LU) today announced that its Base Station Router (BSR) product was selected as the first place winner of a CTIA WIRELESS 2006 Wireless Emerging Technologies (E-tech) Award in the category of "Most Innovative In-Building Solution." Award recipients were announced yesterday in a ceremony at the Las Vegas Convention Center during the CTIA WIRELESS trade show.

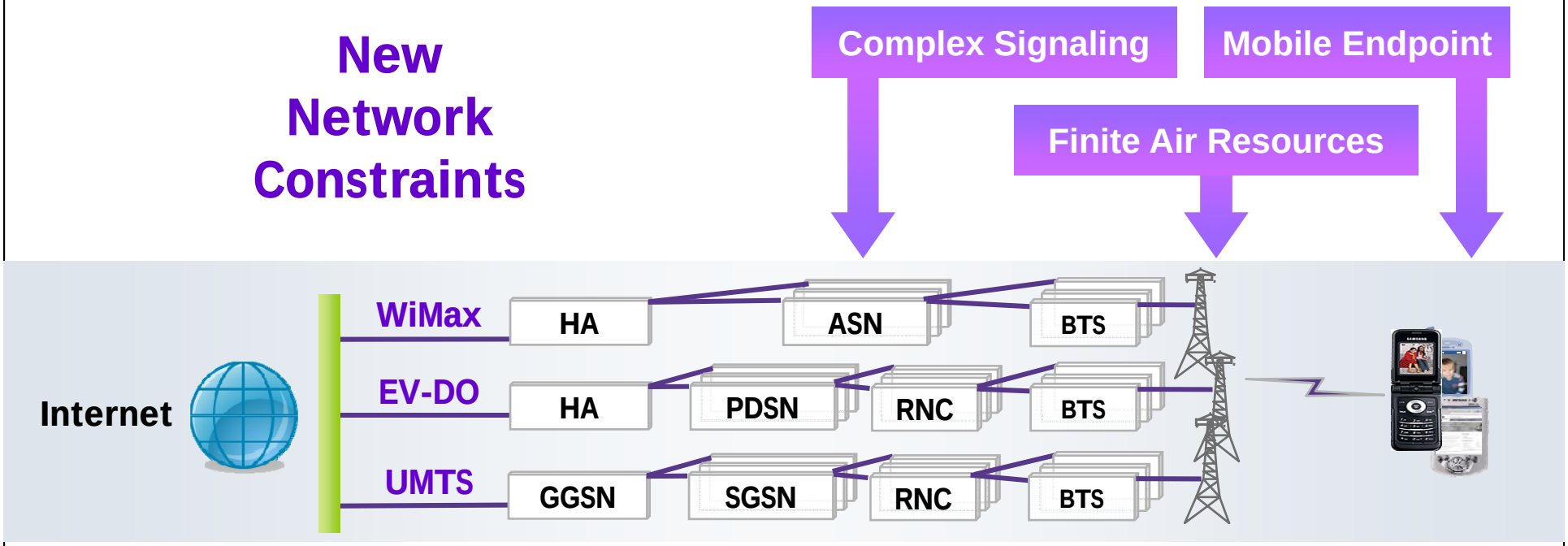
The Wireless E-tech Awards program is designed to give industry recognition and exposure to the best wireless products and services in the areas of Consumer, Enterprise and Network technology. Nearly 200 applications were submitted and reviewed by a panel of recognized members of the media, industry analysts and executives, as well as select show attendees. Products were judged on innovation, functionality, technological importance, implementation and overall "wow" factor.

Enabling Technologies

- Future Telecom Networks will need secure, quality-enabled, high-speed, and well-managed converged packet cores
- Bell Labs has several breakthrough programs to enable this change. Here are three examples:
  - SoftRouter: A new architecture to deal with increased complexity of data networking
  - Base Station Router: An access router which terminates all radio network processing
  - AWARE System for Wireless DDoS Defense

Wireless Data Networks Subject to Existing and New Types of Attacks

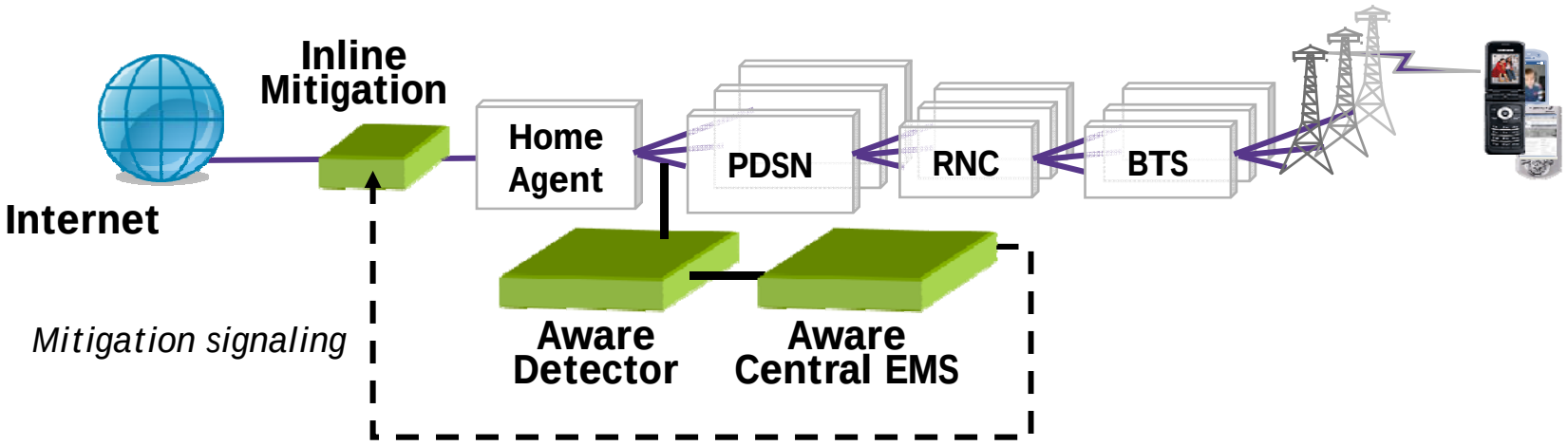
New Network Constraints



New Network Vulnerabilities

Existing IP Threats	New Wireless Threats
• Spam • Virus • Worms • Malware • Phishing • DDoS	• Signaling DoS • Battery Drain • RF DoS • Paging Attacks • Wireless-unfriendly apps (e.g. P2P)

AWARE: A Bell Labs 3G/4G Wireless Security Solution



- AWARE Detector is a behavioral-based packet inspection engine with algorithms tuned to the specifics of the wireless network architecture & protocols
- We have developed algorithms based on traffic profiling and statistical models that can detect low volume wireless DoS attacks
- The system detects and mitigates traffic that will cause RNC signaling overload, unnecessary airlink usage, paging overload, and unnecessary subscriber battery drain
  - Mitigation: signaling to inline elements to block unwanted traffic and mobile quarantine to remove infected or malicious mobile from wireless network

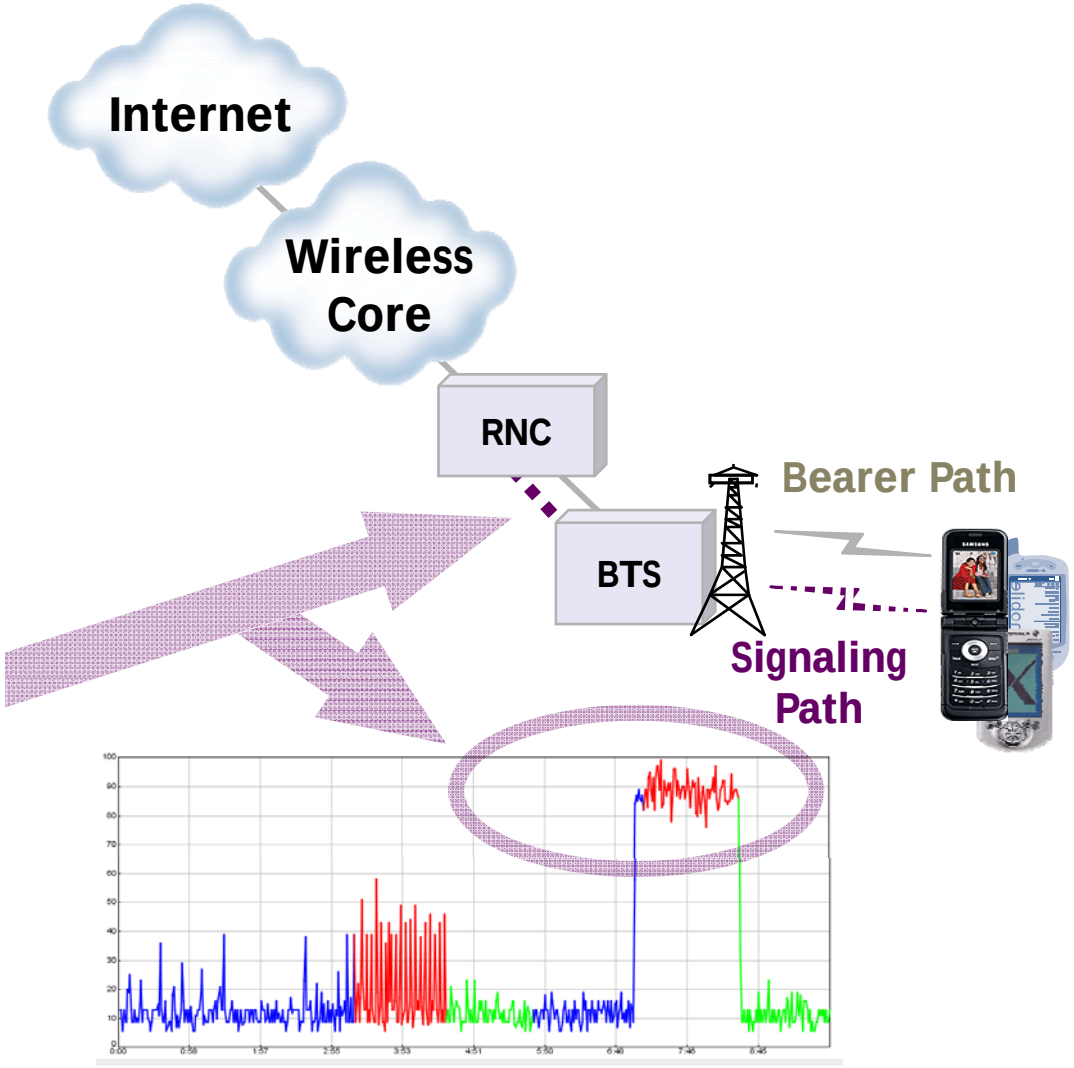
Denial of Service - Signaling Attacks on 3G Networks

Structure of Signaling Overload

- Attack leverages active mobile sessions in the network
- Small amounts of data are sent to re-initiate the session after it is released causing extra signaling load

Impact

- Low-volume attack generates signaling congestion at the RNC
- Overload of the RNC will result in a denial of service to subscribers



Alcatel·Lucent

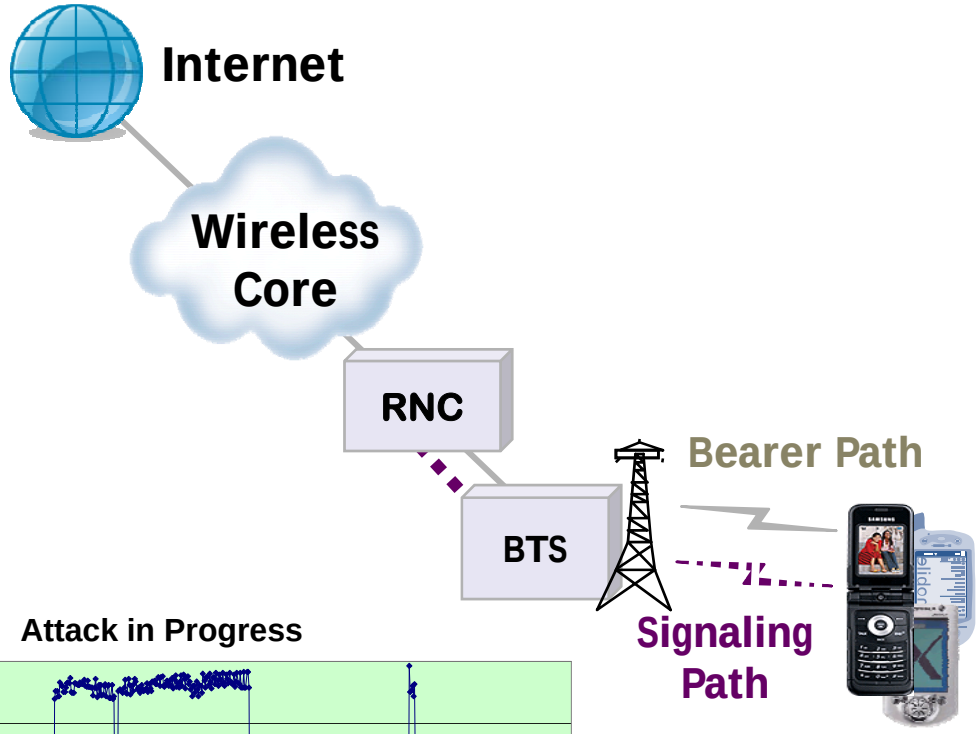
Denial of Service - Battery-Drain and RF Channel Exhaustion

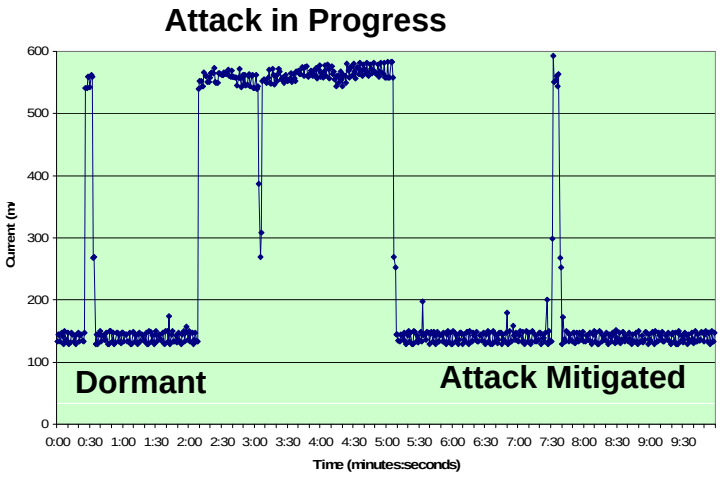
Structure of a Battery-Drain Attack

- Attack leverages active mobile sessions and sends packets to prevent transition to dormancy (e.g., low volume 40 bytes every 10 seconds)

Impact

- Wastes radio resources
- Drains mobile battery

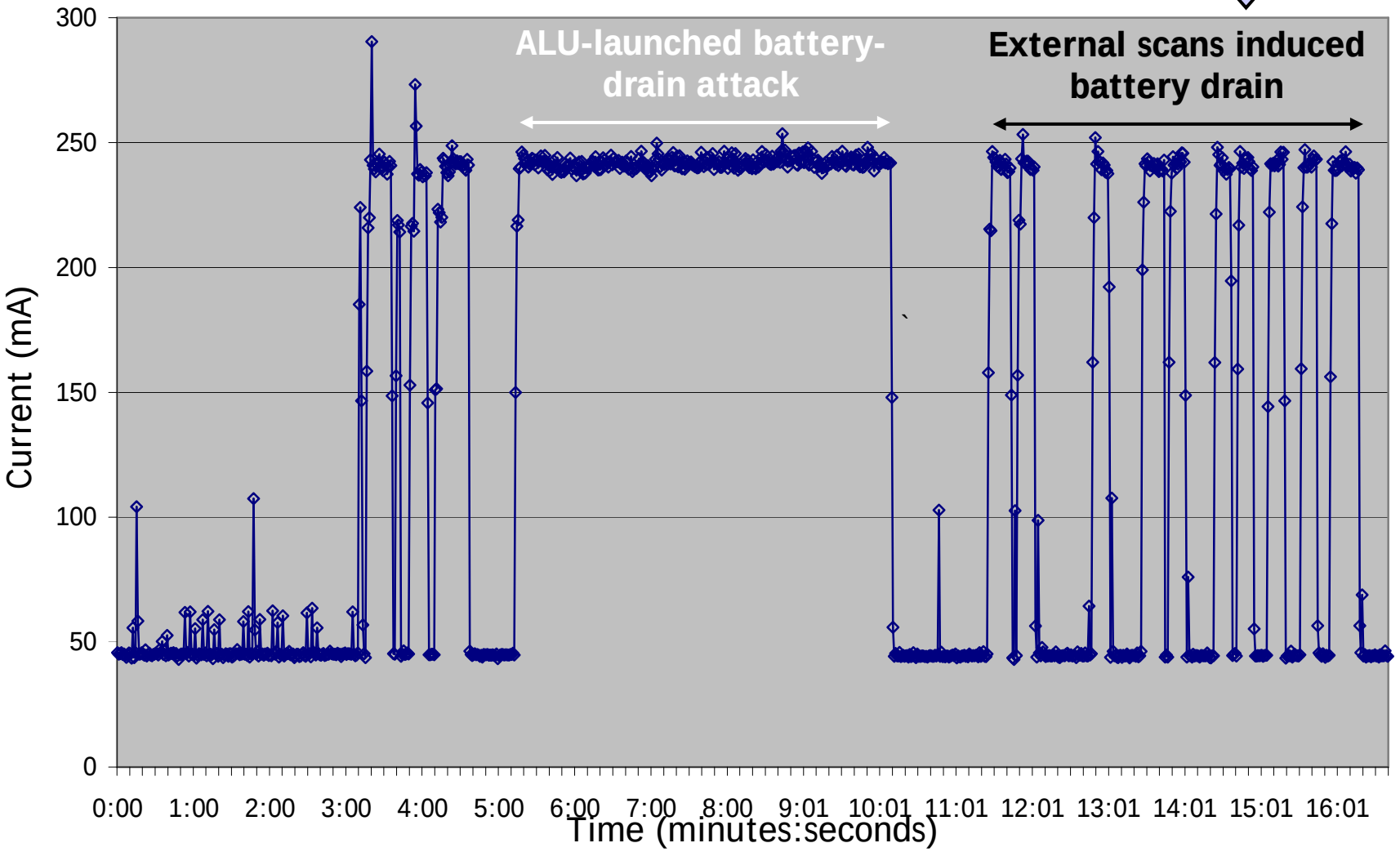




Alcatel·Lucent

Battery Drain on live UMTS Wireless PC Card

Observed affect on energy consumption due to unwanted traffic coming from various Internet sources and other mobiles



Alcatel·Lucent

Recent Abuse Observed on North American Carrier's 3G Network

Detection Evasion: need to identify subscriber not IP address

- Same subscriber's mobile used **24** different IP address when performing scans on other mobiles

One subscriber's abusive behavior:

- Uploaded 1GB / Downloaded 3.5GB
- Communicated with P2P sites - 5k eDonkey & 37k Gnutella sites

Worms and Port Scans (attempt/response)

Result in significant wasted air resources

- Port 135: 10+ different worms (31,213 / 2,326)
- Port 137: Chode worm (135,483 / 2925)
- Port 139: 10+ different worms (59,698 / 4063)
- Port 1026: MS message spam (67,034 / 436)
- Port 5900: install of backdoor program, (96,159 / 2,380)
- Mobile scanner: scans 4426 mobiles on 6 different ports

Malfunction Device Impact on Wireless Network:

- One 3G network was continuously experiencing Denial of Service overloads due to a malfunctioning air card
- Several man-months were required to identify the device

Conclusions

- Multimedia content is the major driver for next-gen networks.
- These networks have to be QoS-enabled, reliable, secure, and manageable.
- Bell Labs has several programs to enable the mobile networks of the future: SoftRouter, Base Station Router, and AWARE DDoS System.
- Mobile networking has a truly exciting future.