

# **Real-time Services over an IP/MPLS network**

Siroos Afshar and Bur Goode  
AT&T



# Outline

---

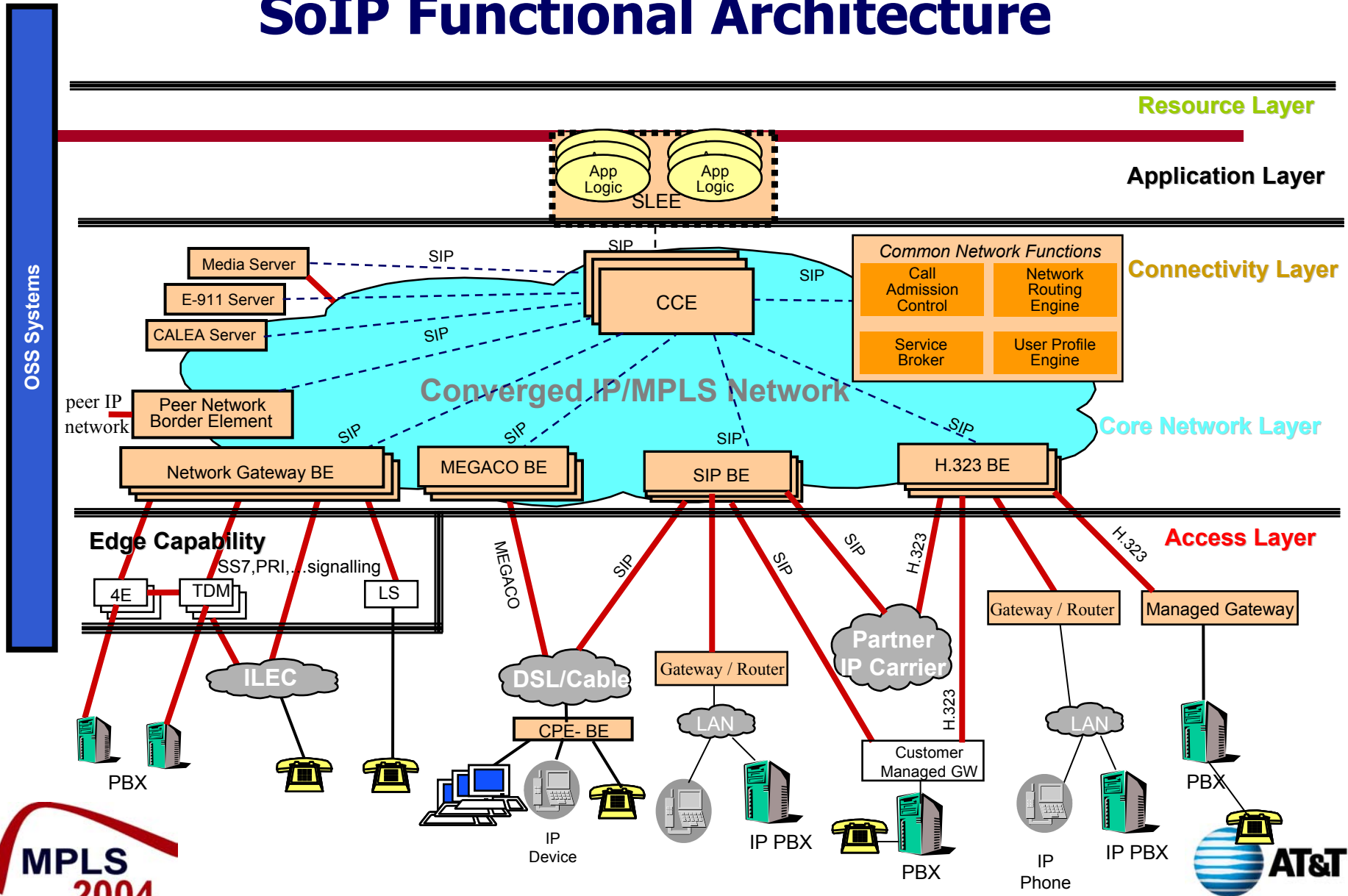
- Objectives of AT&T Architecture
- SoIP Functional Architecture
- Border Element Responsibilities
- SoIP over MPLS VPN (example)
- Performance and Security
- Services over IP
- Conclusions

# Objectives of AT&T Architecture

---

- Carry all services over IP/MPLS network.
- Develop and deploy real-time services (SoIP).
- Maintain high quality and availability.
- Achieve low cost of operations and maintenance.
- Support security for customers and for AT&T.
- Support all popular access technologies:
  - TDM, ISDN (PSTN)
  - ATM, FR
  - PPP
  - Ethernet

# SoIP Functional Architecture



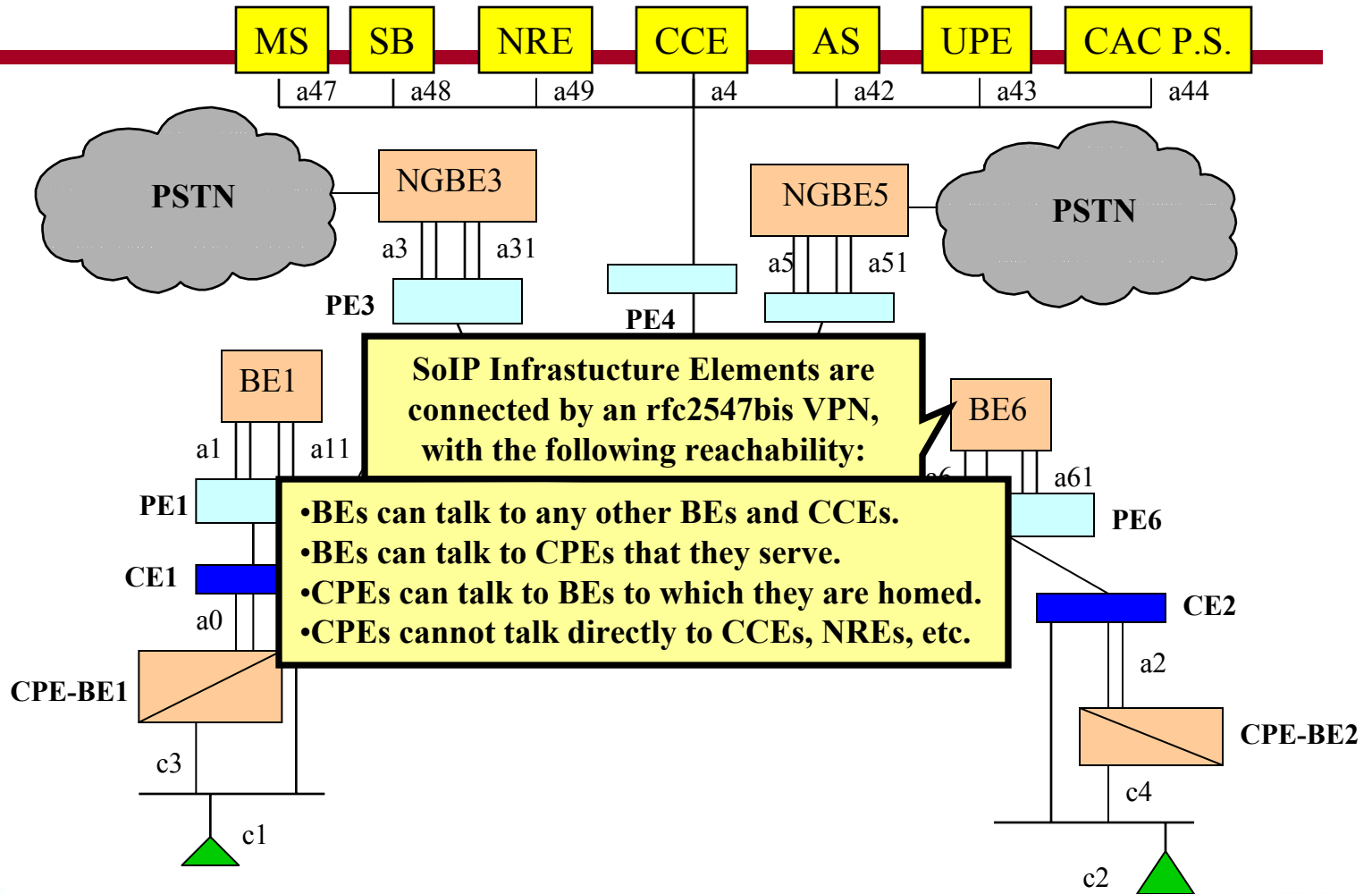
# Border Element Responsibilities

---

- **BE is the boundary of trust for AT&T SoIP Network.**
- **BE Functions:**
  - Interface with CCE for all call control functions.
  - Provide protocol conversion between SIP and the access protocol (H.323, MGCP, SS7, ISUP, CAS, ISDN, etc.)
  - Provide media transfer and control, including mid-call trigger detection.
  - Provide mgmt/network control of signaling and media streams into VoIP network
  - Provide fault isolation
  - Hide AT&T SoIP Network from customers for security and allow changes internal to network without affecting customer configuration, enforcing security and privacy.
  - Support registration and call admission control.

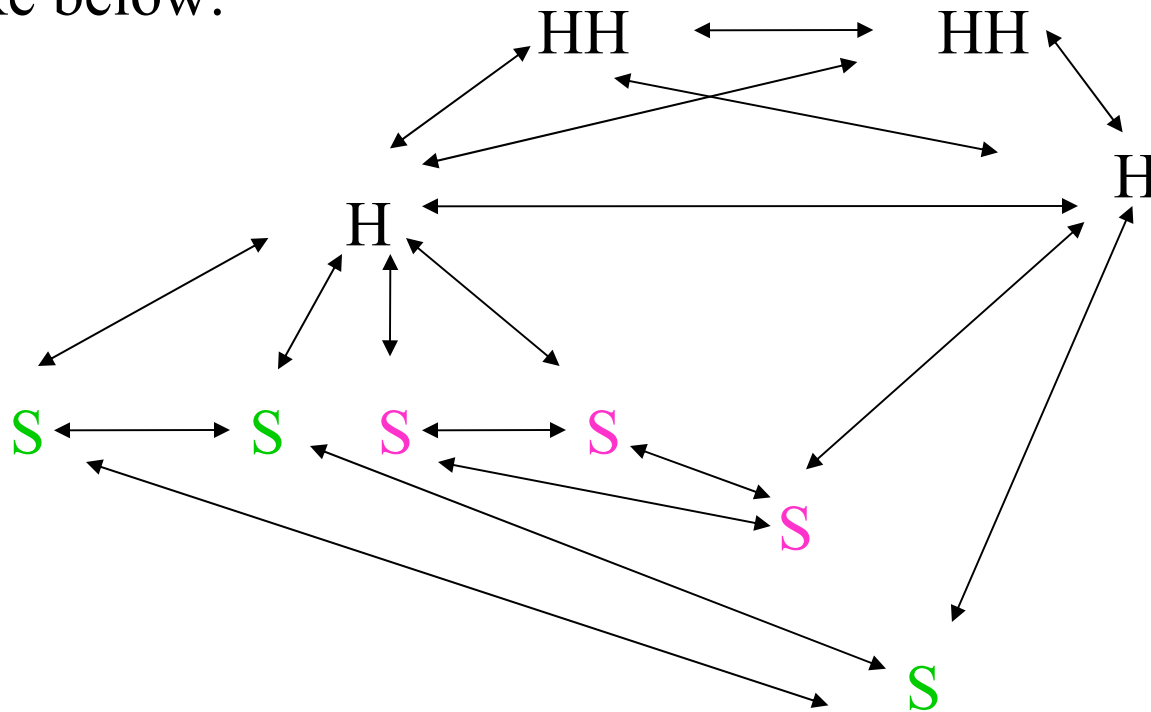


# SoIP over MPLS VPN



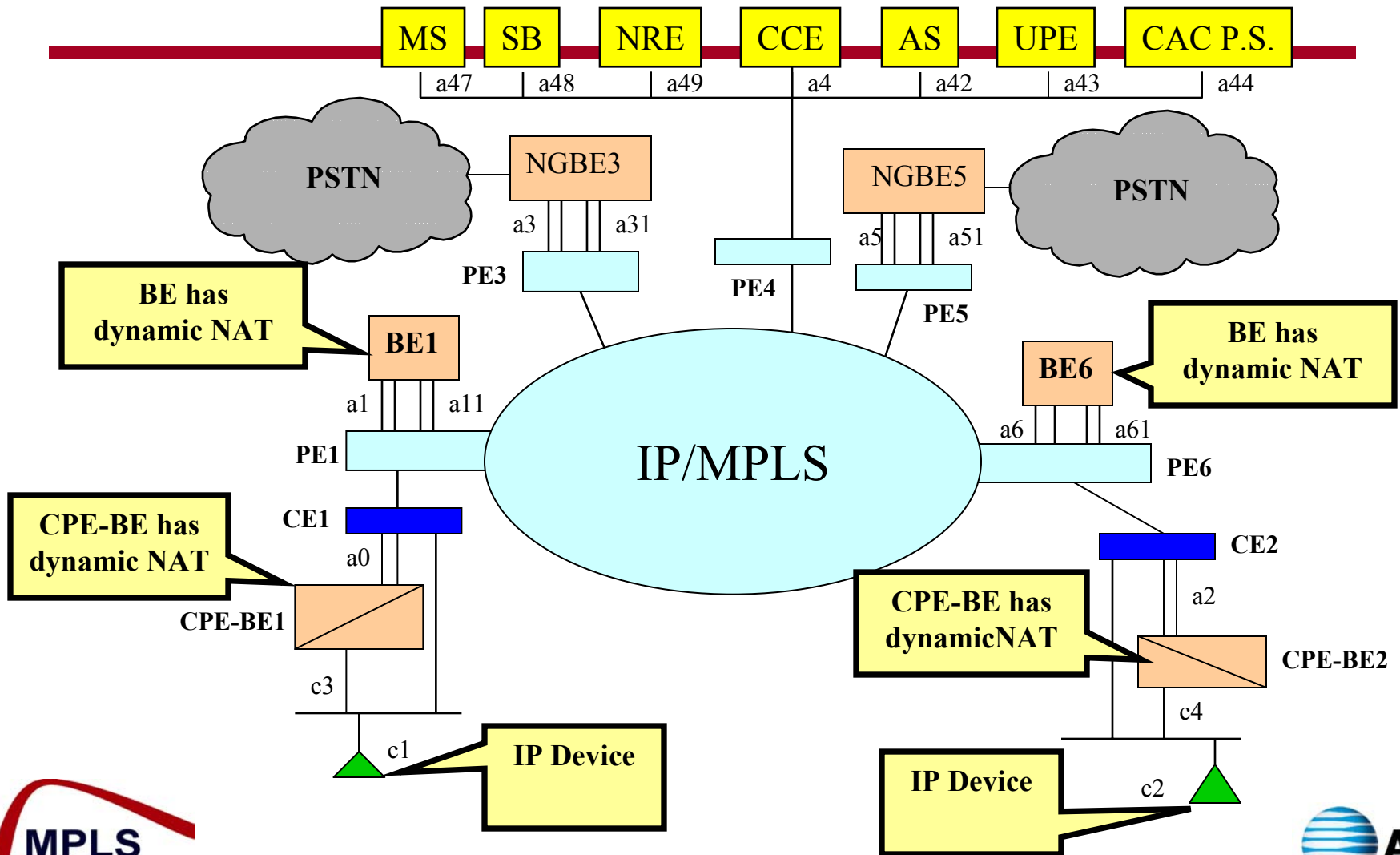
## SoIP Reachability Topology for MPLS VPN Services

- If we use notation HH for CCEs/NREs etc.. H for BEs and S for CPEs (with color coding for VPN). Reachability topology looks like below:

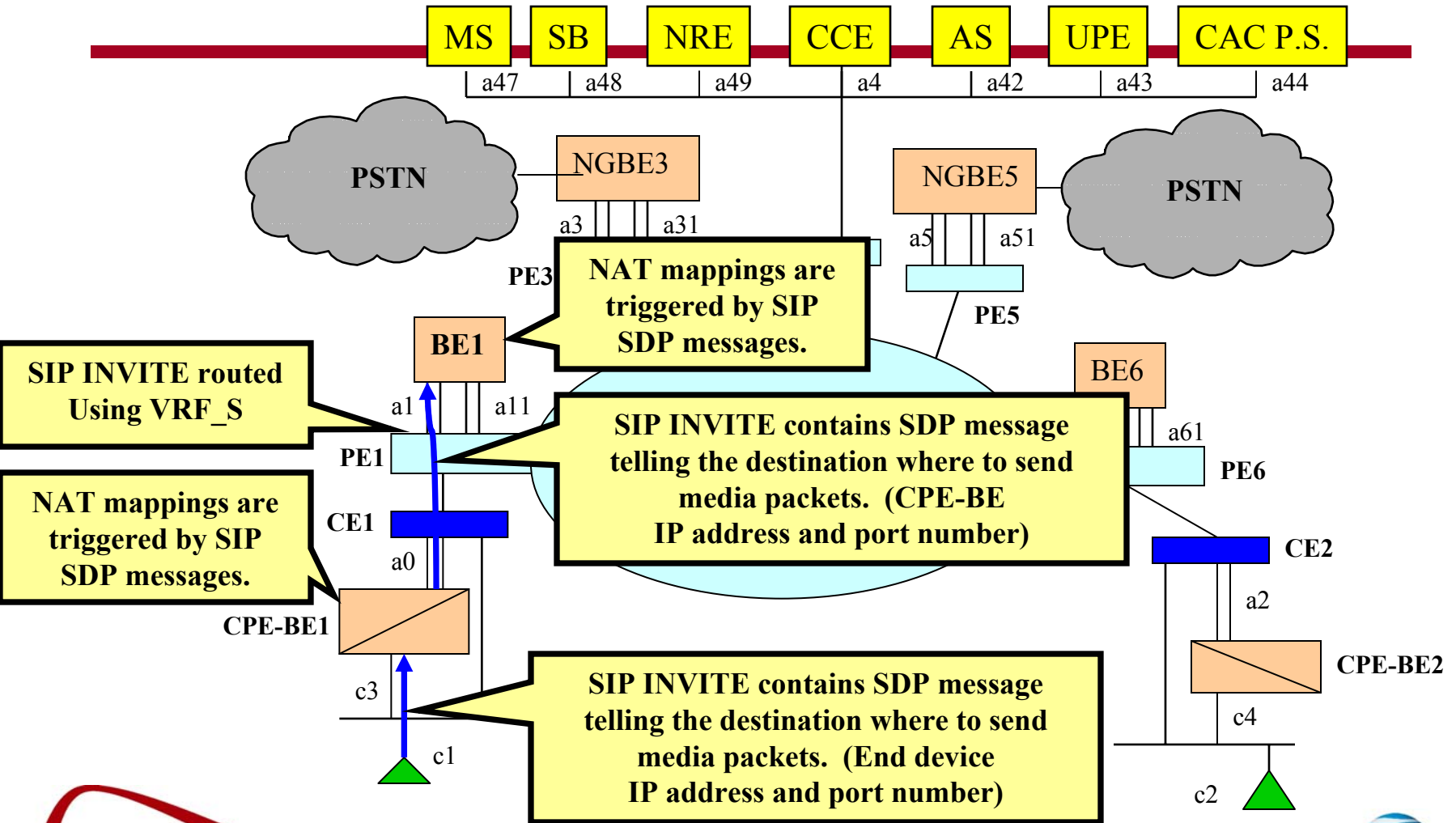




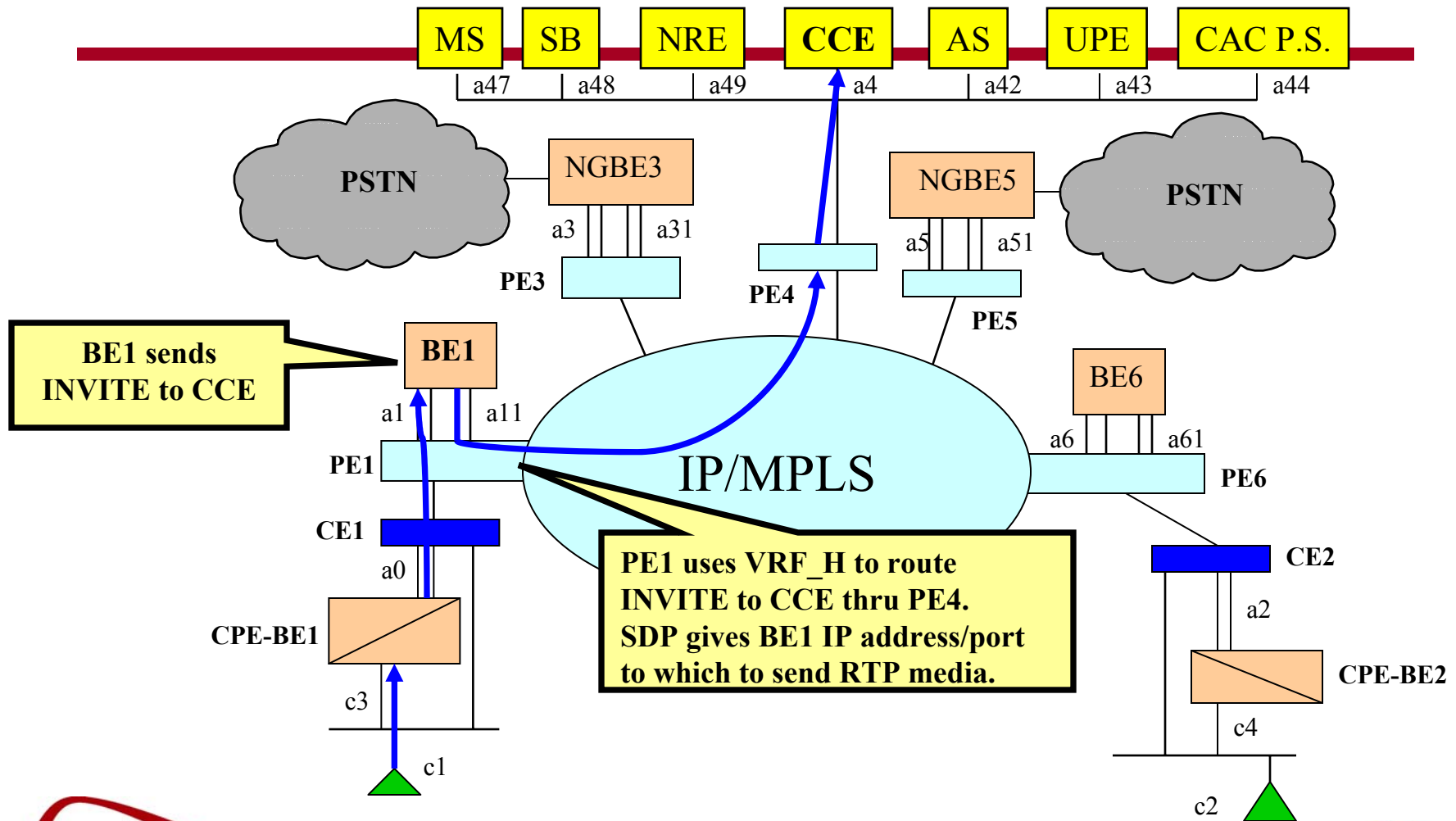
# SoIP over MPLS VPN



# SoIP over MPLS VPN



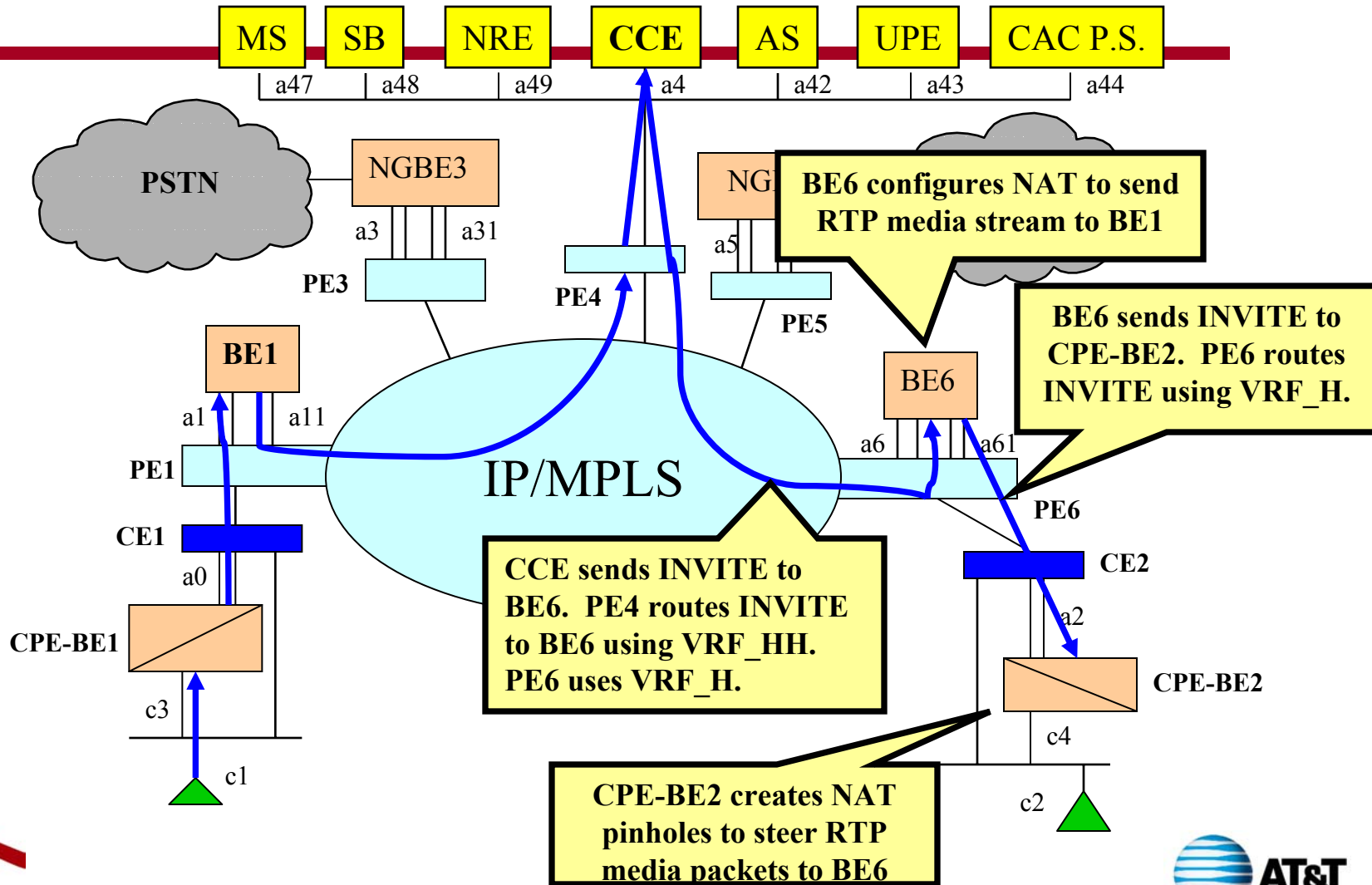
# SoIP over MPLS VPN



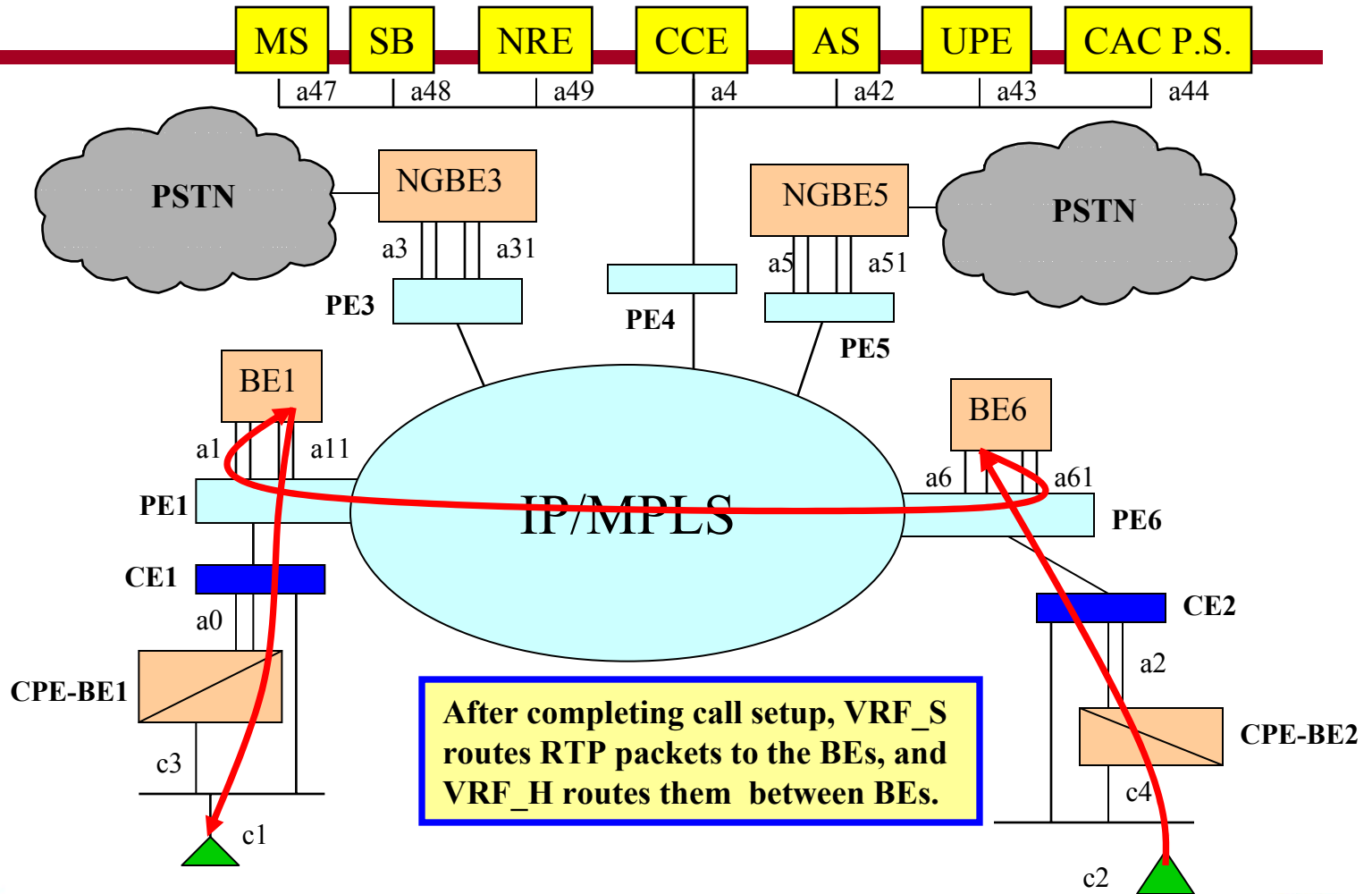
BE1 sends INVITE to CCE

PE1 uses VRF\_H to route INVITE to CCE thru PE4. SDP gives BE1 IP address/port to which to send RTP media.

# SoIP over MPLS VPN



# SoIP over MPLS VPN



# Performance and Security

---

- COS/QoS -- marking at edge & several queues in core
  - Real-Time
  - High Performance Data
  - Medium Performance Data
  - Best Effort
- Resilient to known security threats
  - Preserves confidentiality of customer communications.
  - Preserves availability and integrity of SoIP service.
    - Shields from DDOS attacks.
  - Prevents theft of service.

# Services over IP

---

- SoIP Connectivity Layer provides all network primitives needed to implement services.
- Services enabled by Connectivity Layer
  - Basic media services
  - E-911
  - Lawfully Authorized Electronic Surveillance (LAES)
  - Call Detail Recording
- Connectivity Layer provides a unified, shared environment that supports new services and access technologies without changing the infrastructure.

# Conclusions

---

- AT&T SoIP Architecture facilitates development and deployment of new as well as traditional services over AT&T IP/MPLS network.
- MPLS VPN facilitates security of SoIP Infrastructure
  - Border Elements provide boundary of trust, interfacing with CPE and other service providers to steer authorized packets through SoIP Infrastructure.
  - BEs are connected together in an MPLS VPN using special VRFs in the PE routers.
- With high performance, reliability, availability and scalability, the AT&T SoIP Architecture provides a growth platform for voice and multimedia services of the future.



# Glossary

---

- BE = Border Element
- CCE = Call Control Element
- CE = Customer Edge (Router)
- CPE = Customer Premises Equipment
- MS = Media Server
- NGBE = Network Gateway Border Element
- NRE = Network Routing Engine
- PSTN = Public Switched Telephone Network
- RTP = Real Time Protocol
- SB = Service Broker
- SIP = Session Initiation Protocol
- SLEE = Service Logic Execution Environment
- SoIP = Services over IP