Exceed with COLT

NGN Architectures, VoIP Security and Protocols

UKNOF 5 25/10/06

Neil J. McRae – Director of Network Architecture

Nico Fischbach – Head of Network Security

COLT Telecom Group

Agenda

What is VoIP?

VoIP Architectures

VoIP Protocols & Security Concerns

Questions

COLT and VoIP

COLT Telecom

> Voice, Data and Managed Services, Tier 1 ISP in EU

> 14 countries, 60 cities, 50k business customers

> 20 000 km of fibre across Europe + DSL

VoIP "experience"

> 3 major vendor directions

  – One "we're coming from the TDM world"

  – One "we're coming from the IP world"

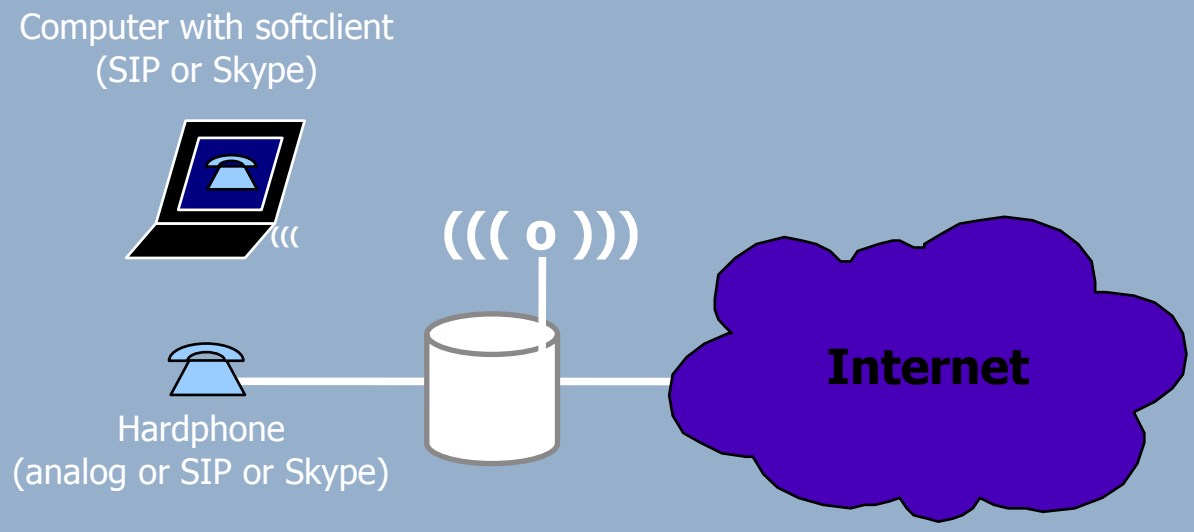
  – One "we're a VoIP company"

> Internet and MPLS VPN-based VoIP services

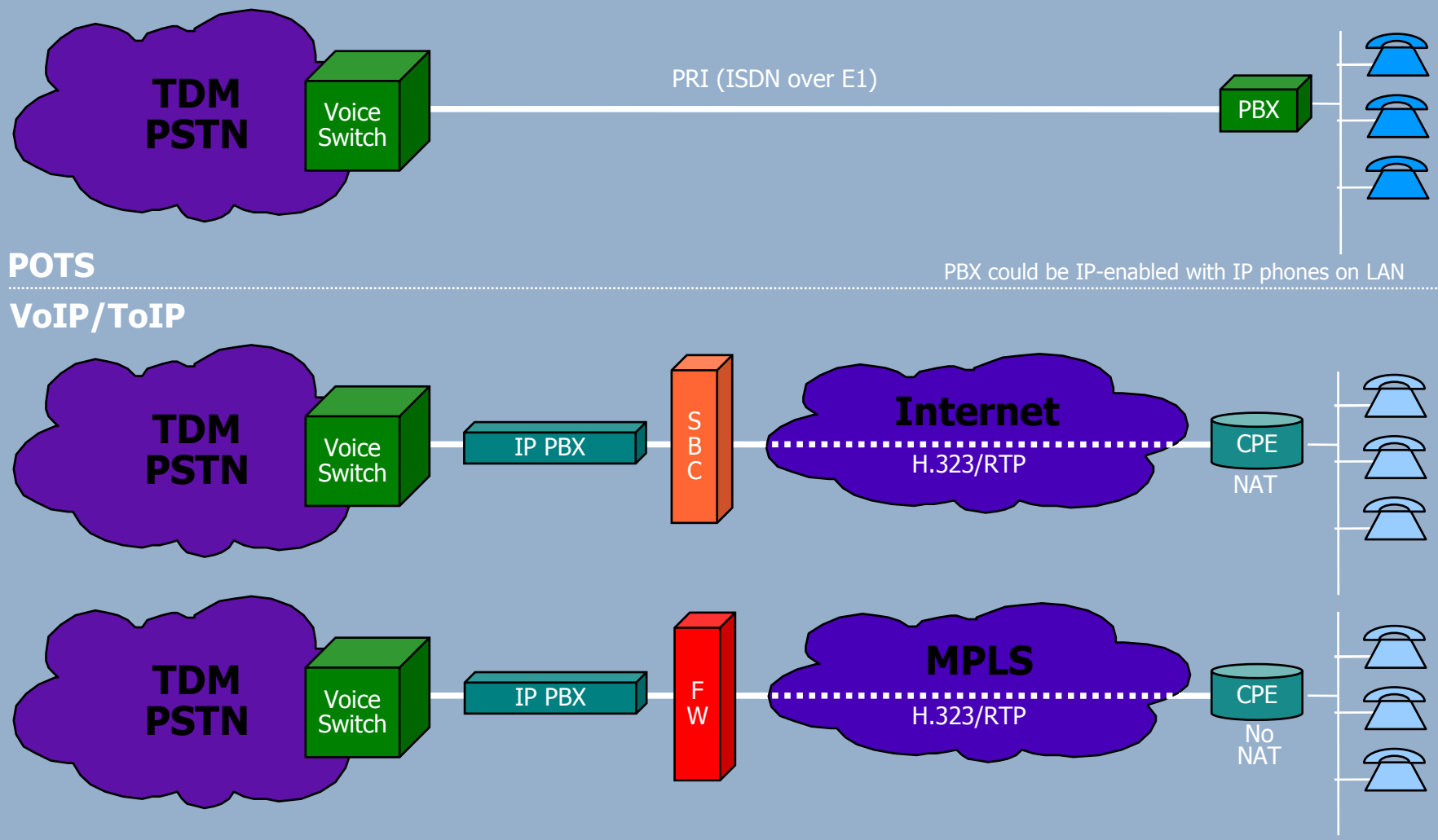
> Own network (fiber + DSL) and wDSL

> Going MSPP + VoIP NGN + IMS – TDM scaling issues

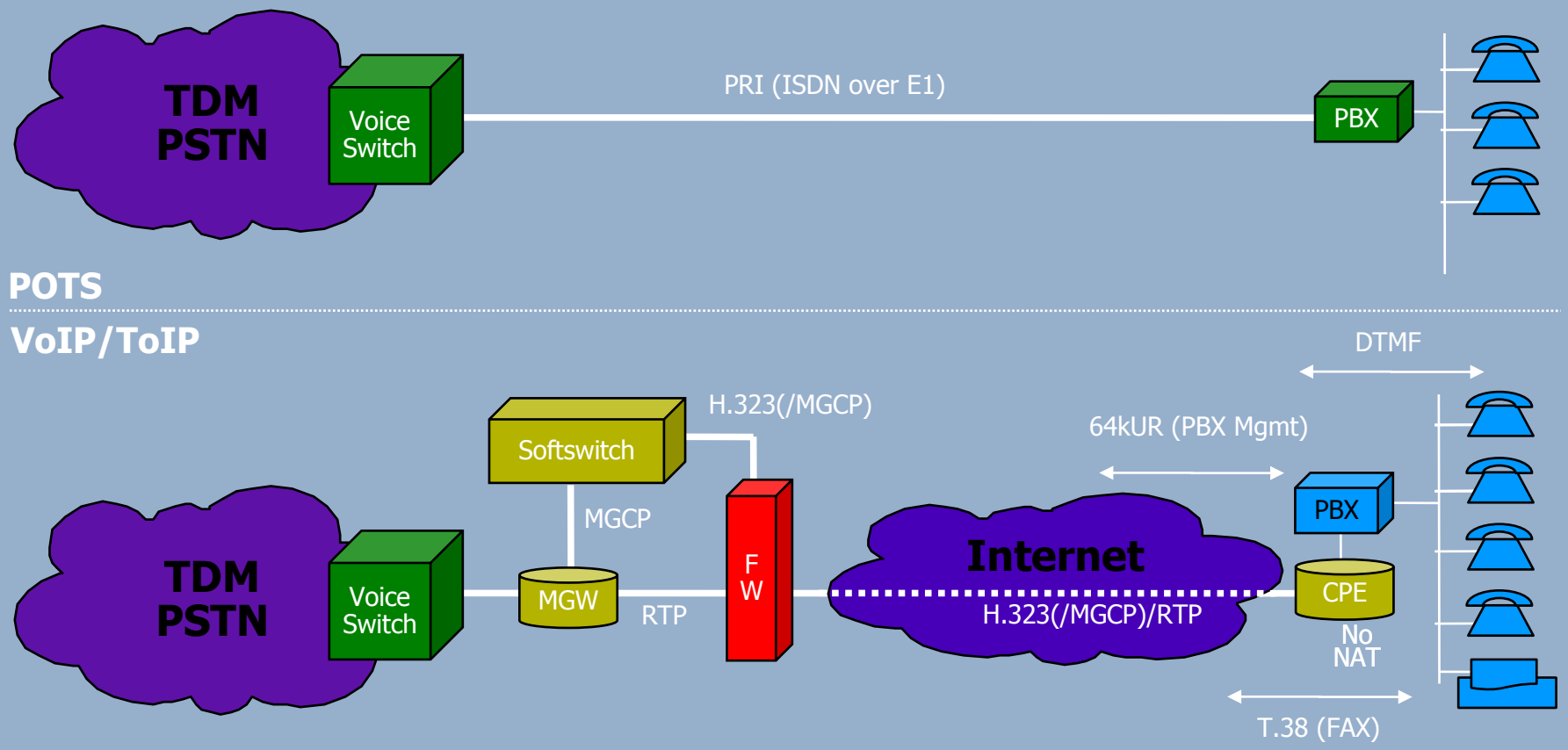
What is VoIP? The Customer Viewpoint



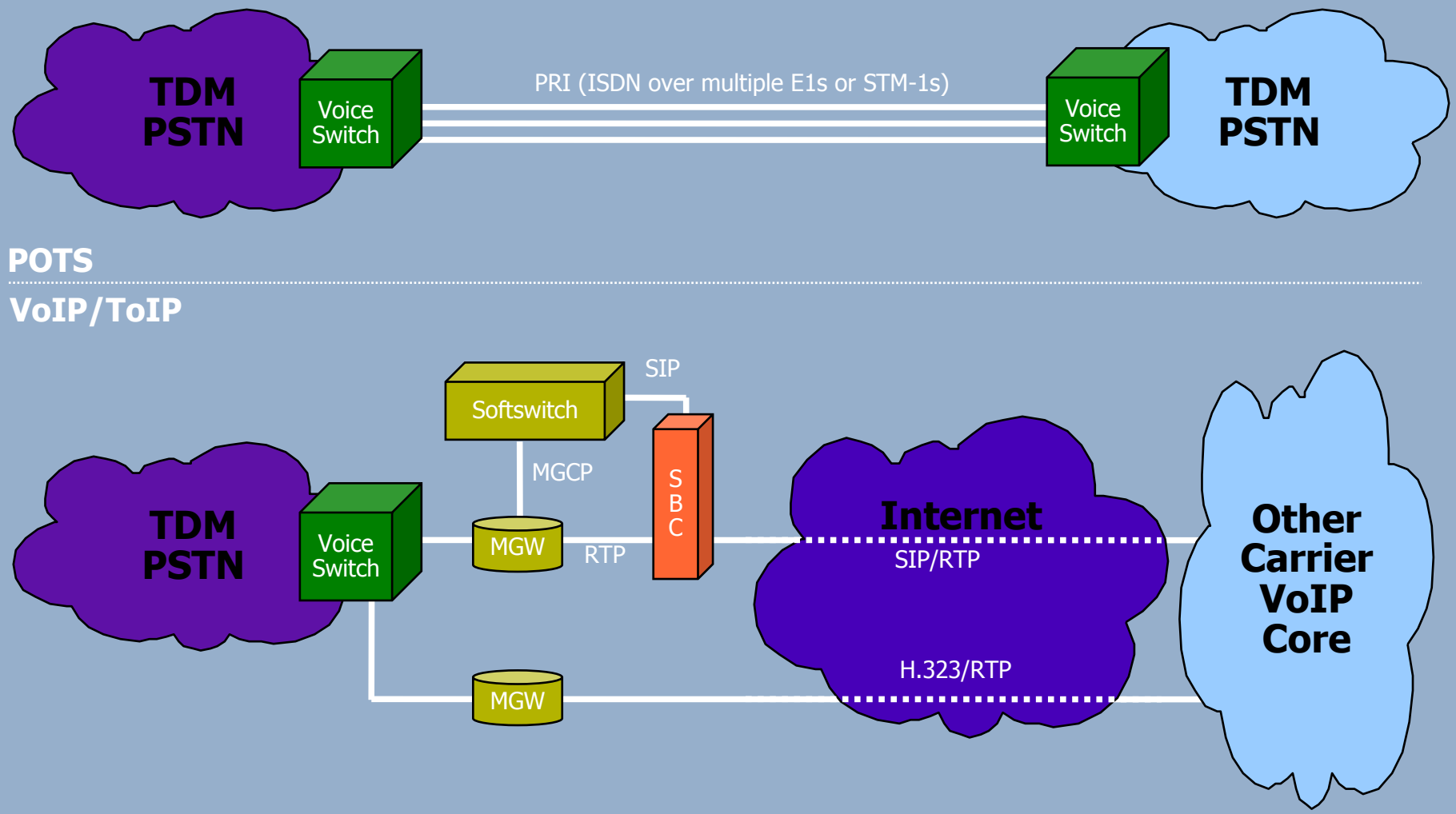
Hosted IP PBX



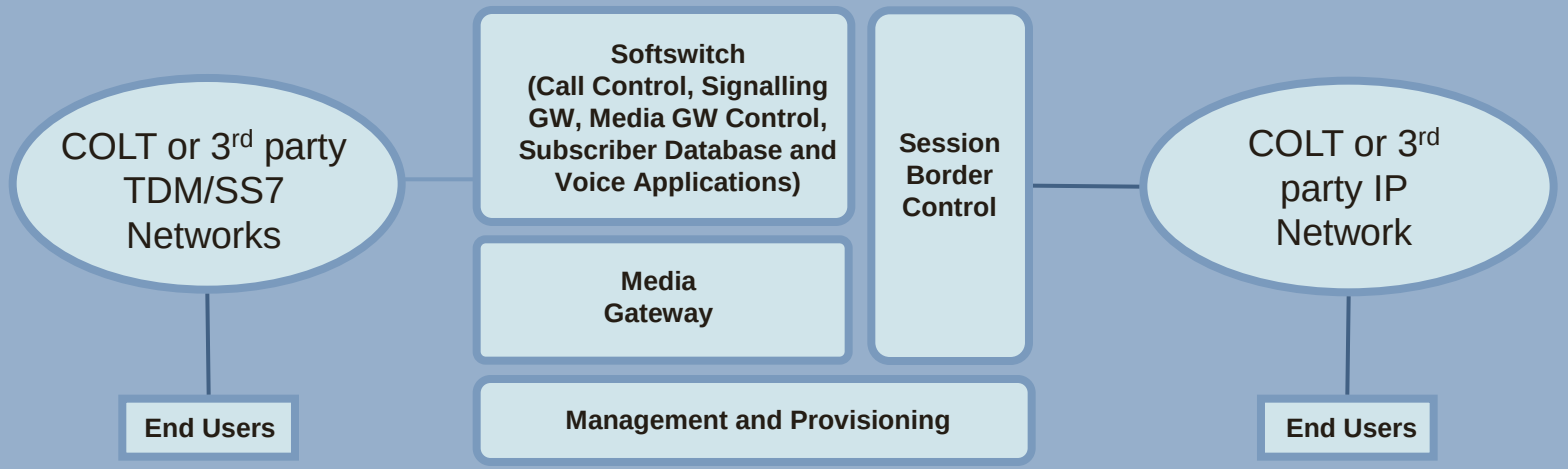
PBX Trunking over IP



Wholesale VoIP

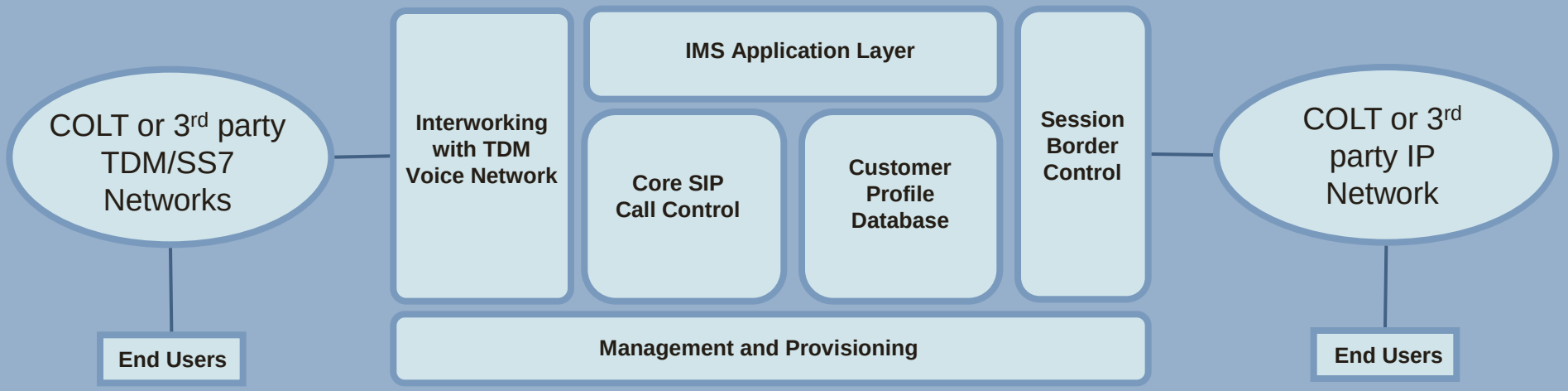


Softswitch Architecture (Intermediate Architecture)



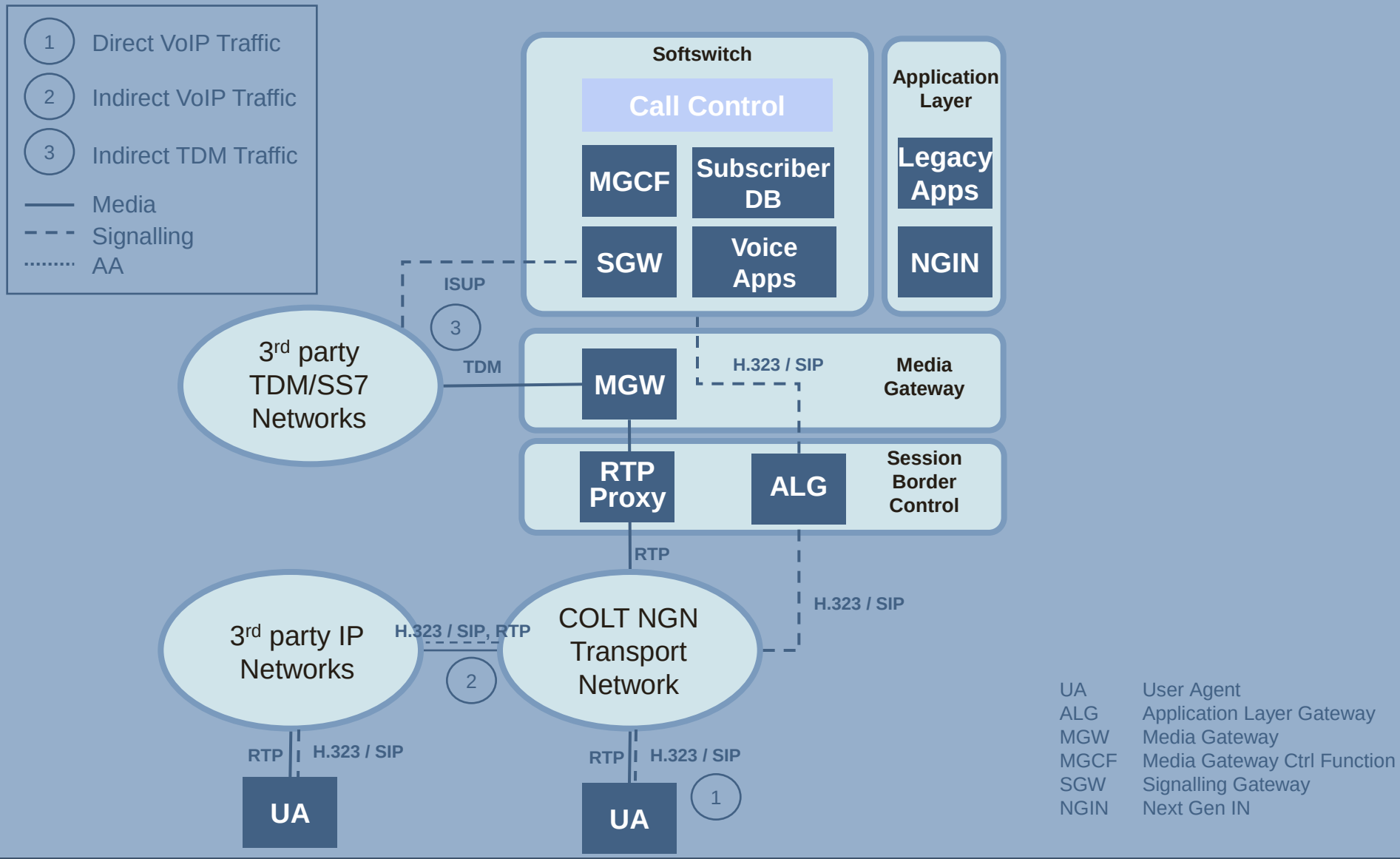
- Softswitch: it combines the Call Control, the Signalling Gateway and the Media Gateway Control function. Together with the Media Gateway function it provides signalling and media inter-working with the legacy TDM voice network. The intelligence of the system (call control functionality) as well the customer database resides within the softswitch function.
- Session Border Control: it provides secure access control to the customer appliances and mediates between the COLT IMS and any 3rd party IP network
- Management and Provisioning: it is an integrated OSS platform that allows end to end provisioning and management across the technology components.

IMS Architecture (Target Architecture)



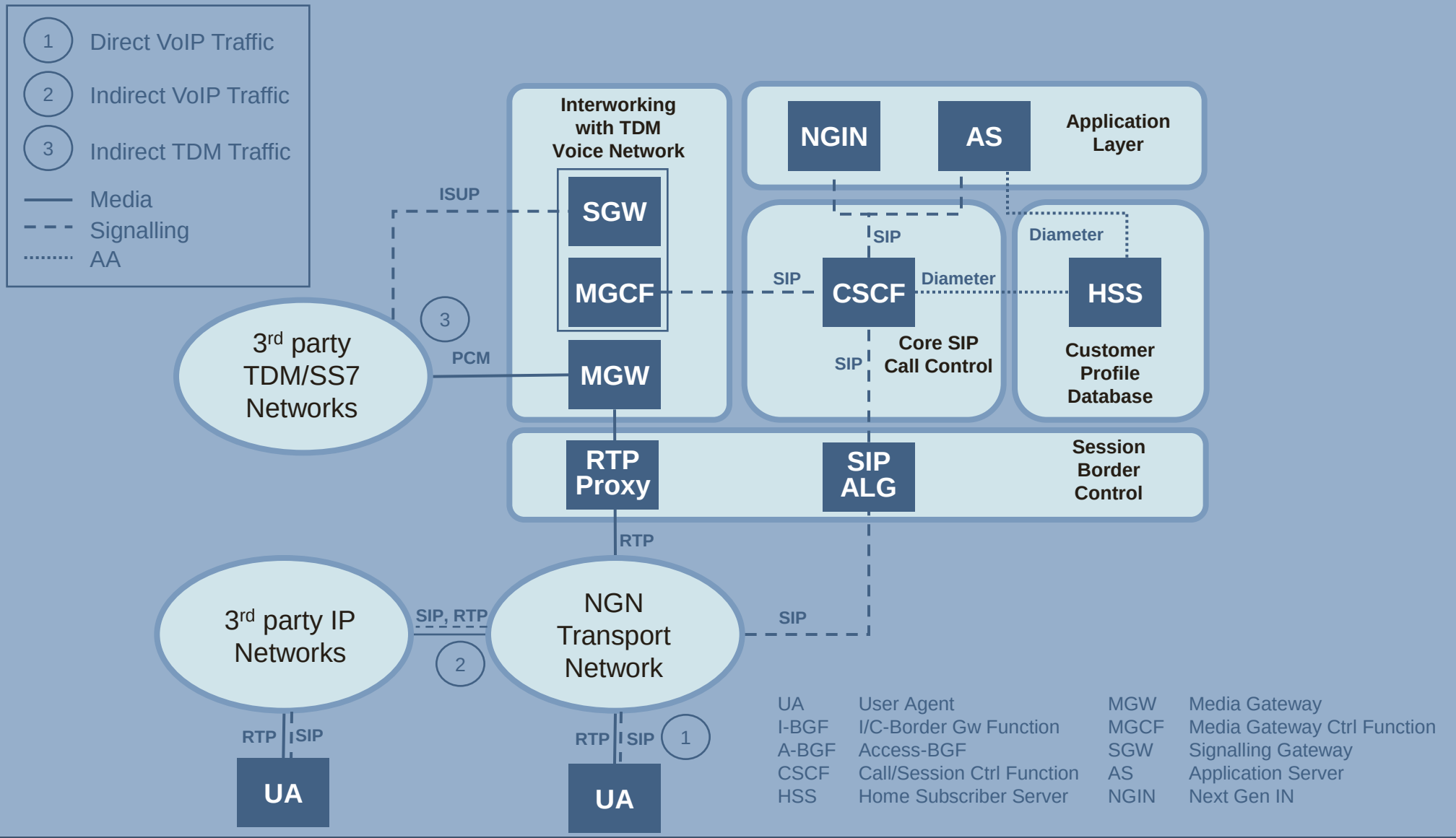
- **Interworking with TDM Voice Network:** it provides signalling and media inter-working with the TDM voice network
- **Core SIP Call Control:** it is a set of SIP enabled devices that control the flow of SIP messages between the customer appliances (IP phones, soft phones, wireless handhelds) and the rest of the IMS components
- **Customer Profile Database:** it contains the user identity and the user service profile, providing session authentication and access to service applications
- **Session Border Control:** it provides secure access control to the customer appliances and mediates between the IMS and any 3rd party IP network
- **Application Layer:** it provides the service logic, with a set of Application Servers dedicated to specific services (eg an IP Centrex AS for telephony services, a Mobility AS for FMC integration, a Messaging AS for unified messaging and presence services)
- **IMS Management and Provisioning:** it is an integrated OSS platform that allows end to end provisioning and management across the IMS technology components.

Softswitch Architecture – Logical Level

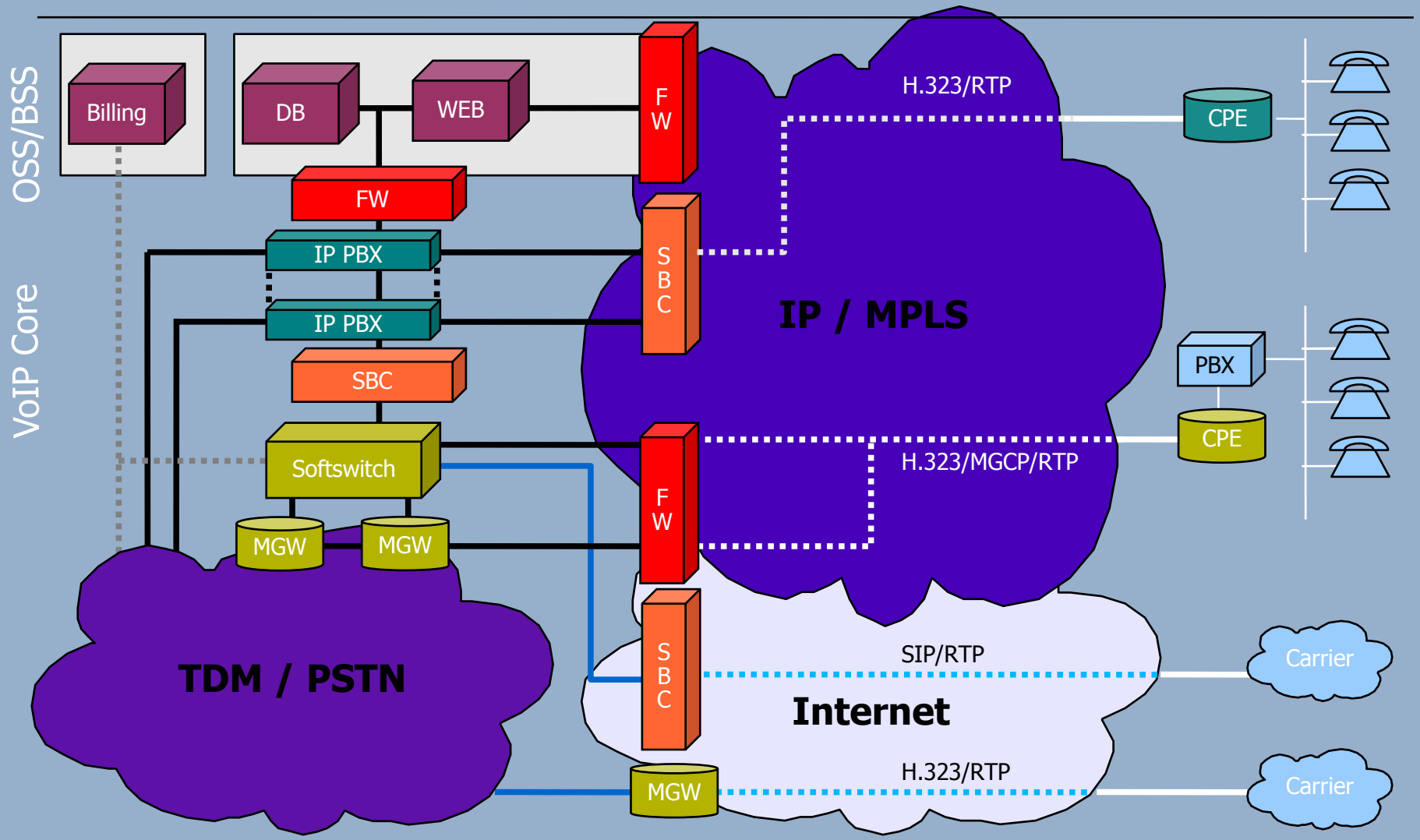


UA	User Agent
ALG	Application Layer Gateway
MGW	Media Gateway
MGCF	Media Gateway Ctrl Function
SGW	Signalling Gateway
NGIN	Next Gen IN

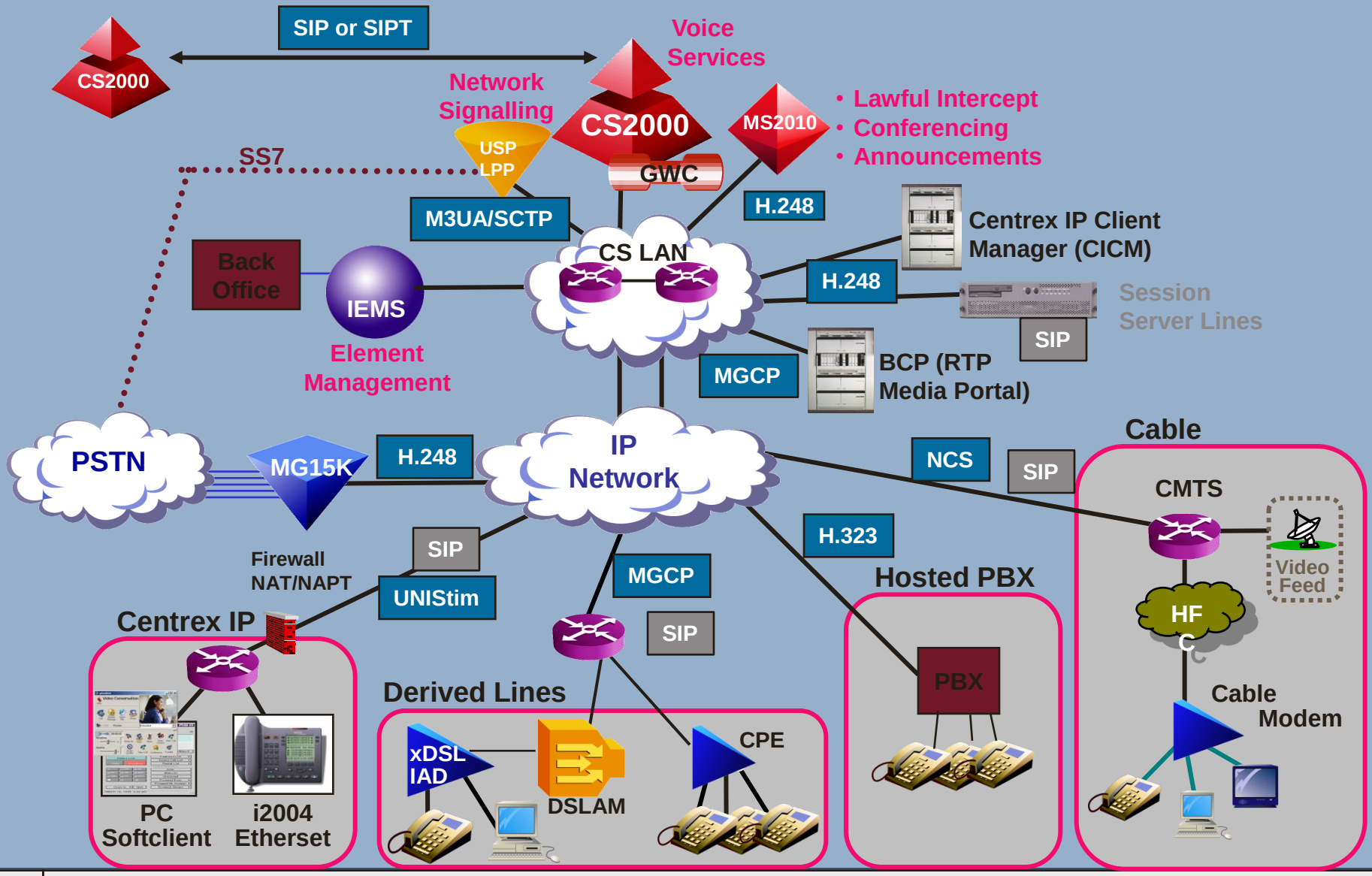
IMS Architecture – Logical Level



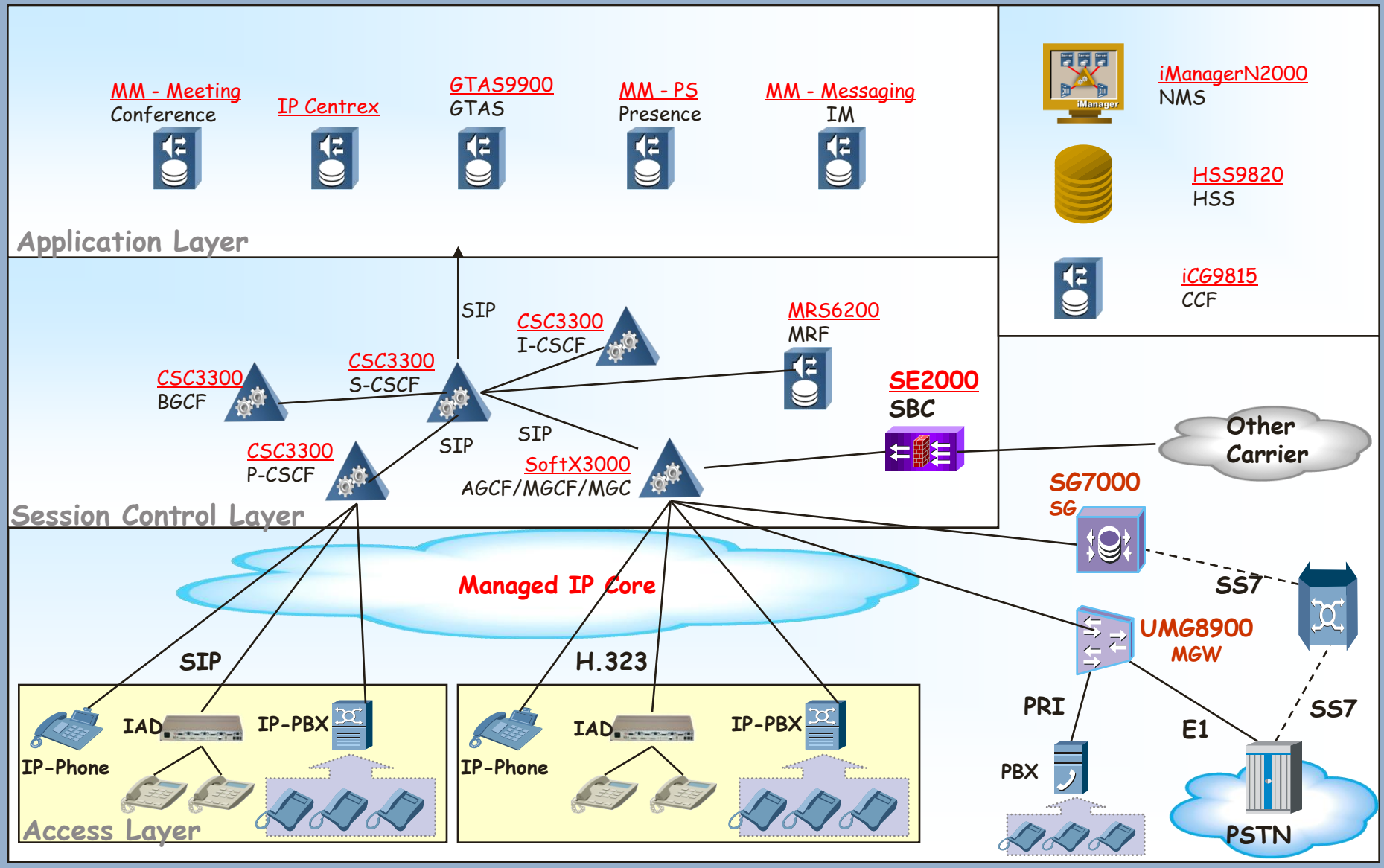
VoIP Core Network Architecture with Security



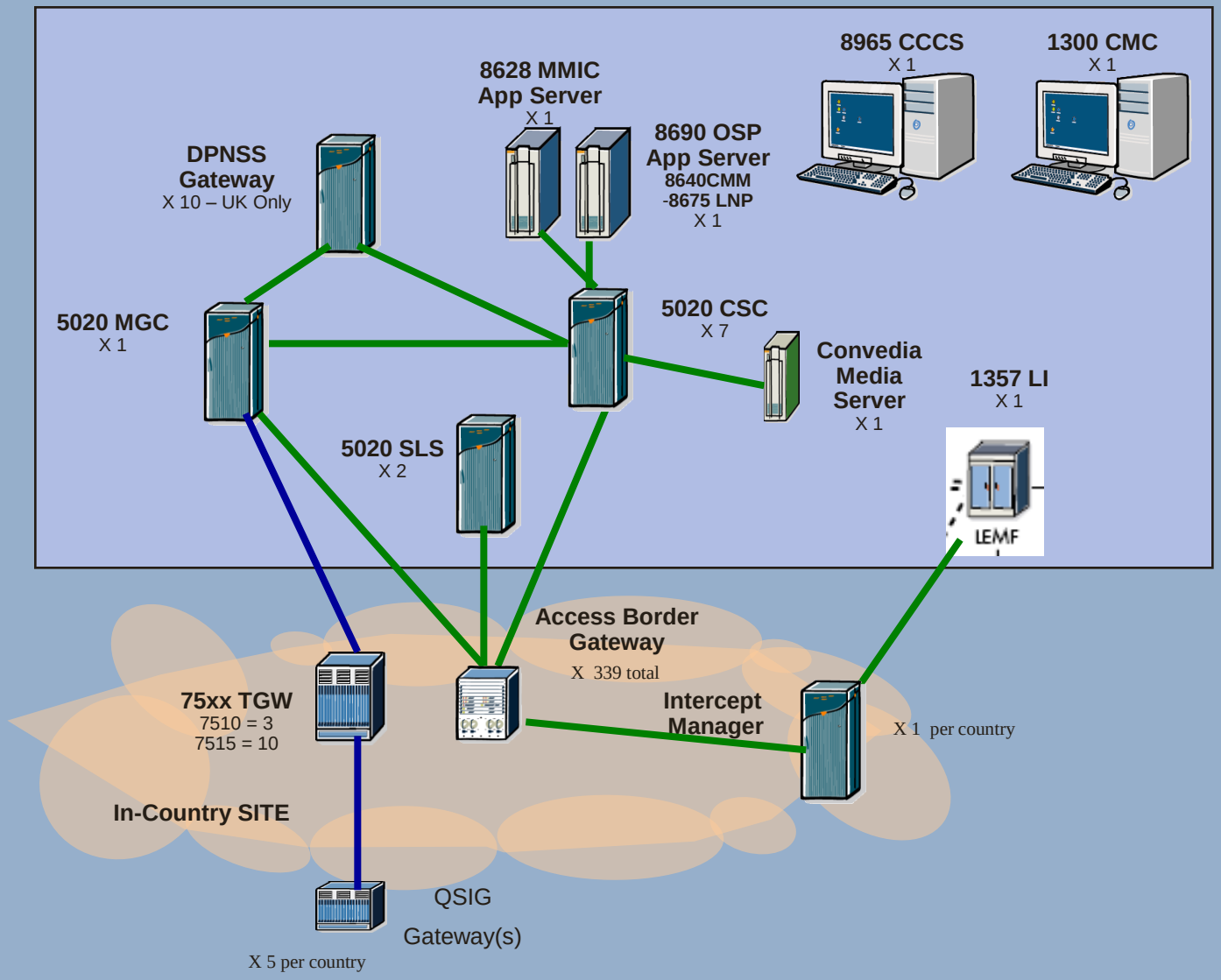
Nortel


SIP or SIPT
CS2000
Voice Services
Network Signalling
USP
LPP
CS2000
GWC
MS2010
• Lawful Intercept
• Conferencing
• Announcements
SS7
M3UA/SCTP
H.248
Centrex IP Client Manager (CICM)
Back Office
IEMS
Element Management
CS LAN
H.248
Session Server Lines
SIP
MGCP
BCP (RTP Media Portal)
PSTN
MG15K
H.248
IP Network
NCS
SIP
Cable
CMTS
Video Feed
HF
C
Cable Modem
H.323
Hosted PBX
PBX
Firewall NAT/NAPT
SIP
UNIStim
MGCP
SIP
Centrex IP
Derived Lines
xDSL IAD
DSLAM
CPE
PC Softclient
i2004 Etherset

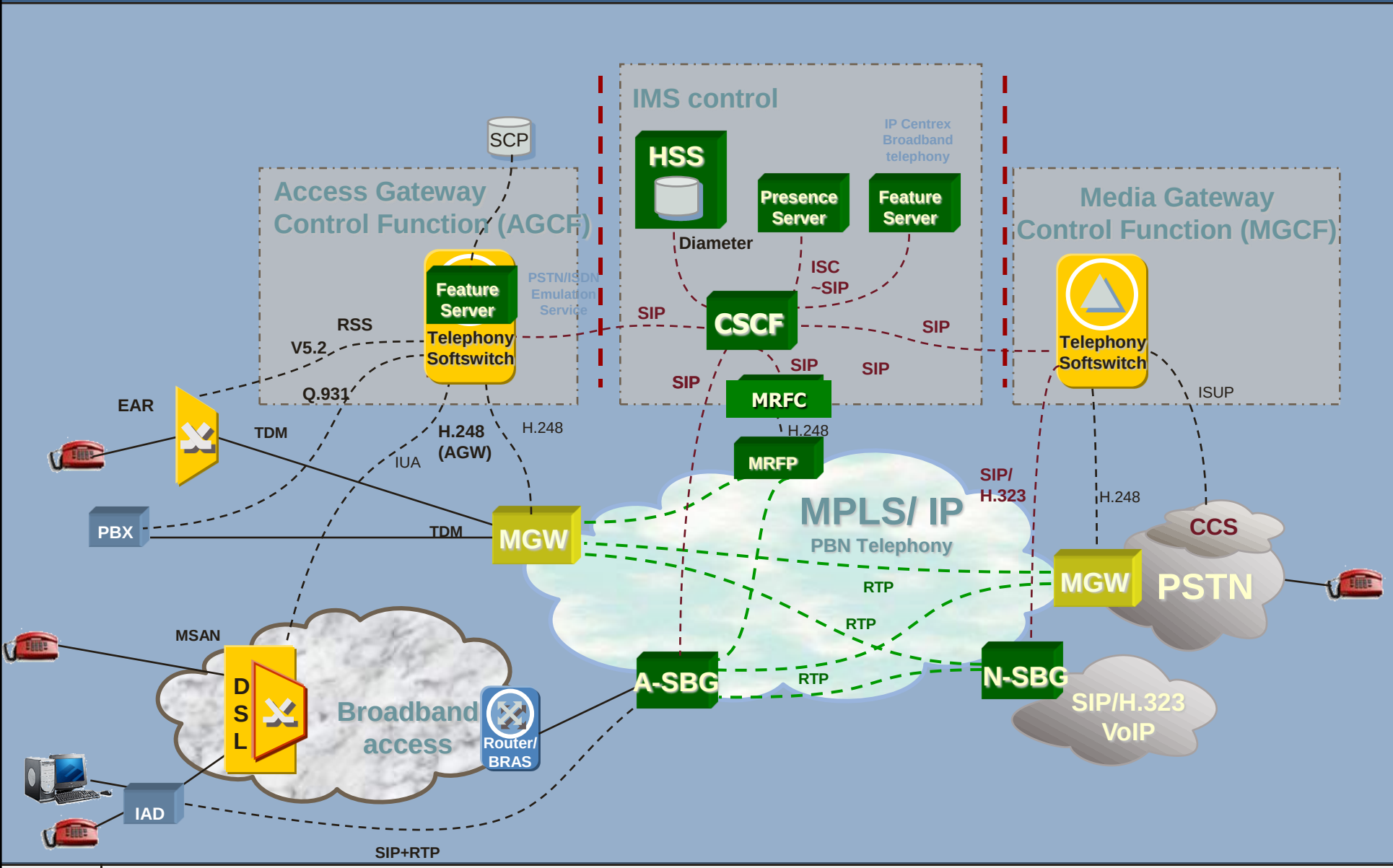
Huawei


MM - Meeting
Conference
IP Centrex
GTAS9900
GTAS
MM - PS
Presence
MM - Messaging
IM
Application Layer
iManagerN2000
NMS
HSS9820
HSS
iCG9815
CCF
SIP
CSC3300
I-CSCF
MRS6200
MRF
CSC3300
BGCF
CSC3300
S-CSCF
SE2000
SBC
SIP
SIP
CSC3300
P-CSCF
SoftX3000
AGCF/MGCF/MGC
Other
Carrier
Session Control Layer
SG7000
SG
Managed IP Core
SS7
UMG8900
MGW
SIP
H.323
PRI
E1
SS7
IP-Phone
IAD
IP-PBX
IP-Phone
IAD
IP-PBX
PBX
PSTN
Access Layer

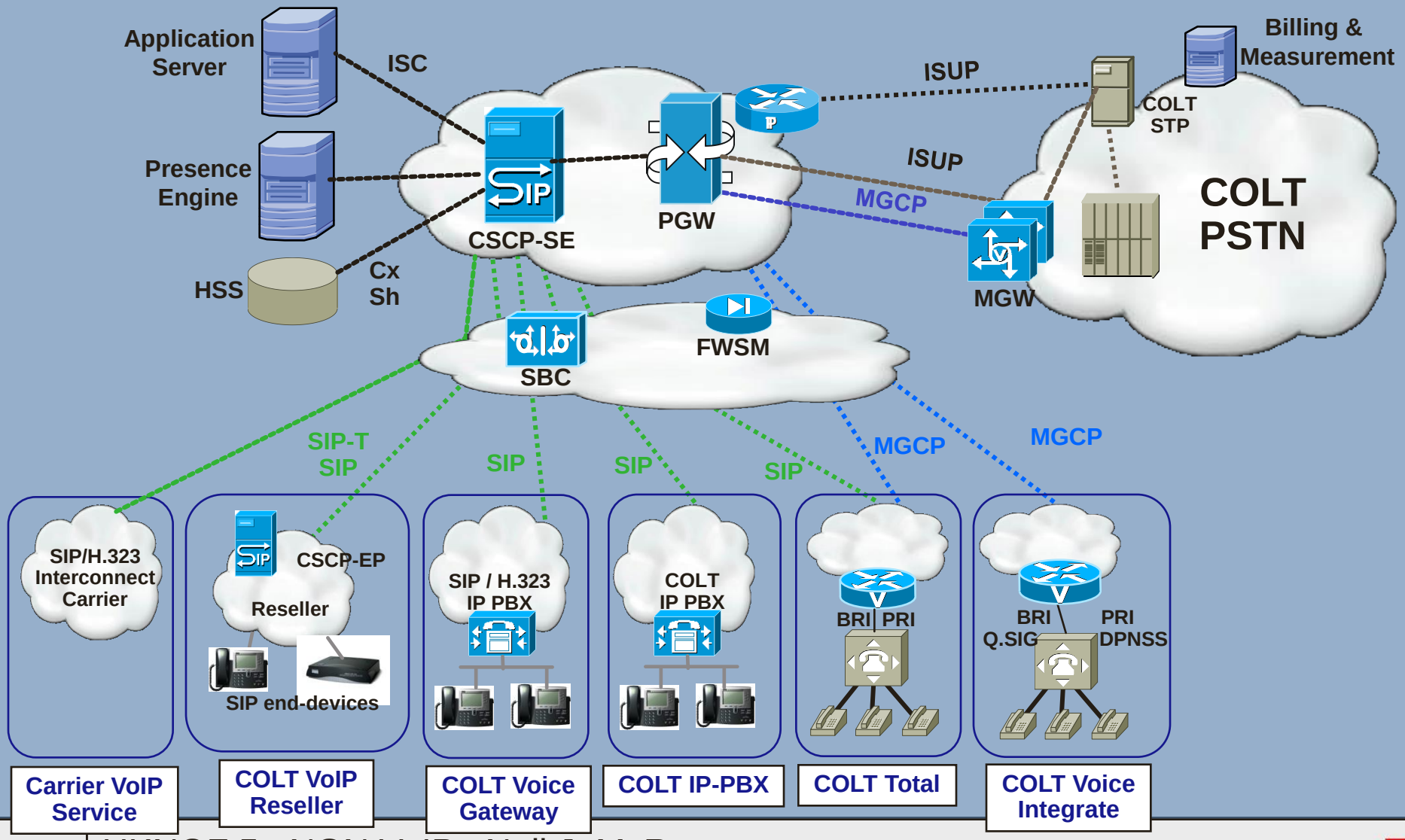
Alcatel


8965 CCCS
X 1
1300 CMC
X 1
8628 MMIC
App Server
X 1
8690 OSP
App Server
8640CMM
-8675 LNP
X 1
DPNSS
Gateway
X 10 – UK Only
5020 MGC
X 1
5020 CSC
X 7
Convedia
Media
Server
X 1
1357 LI
X 1
LEMF
5020 SLS
X 2
Access Border
Gateway
X 339 total
75xx TGW
7510 = 3
7515 = 10
Intercept
Manager
X 1 per country
In-Country SITE
QSIG
Gateway(s)
X 5 per country

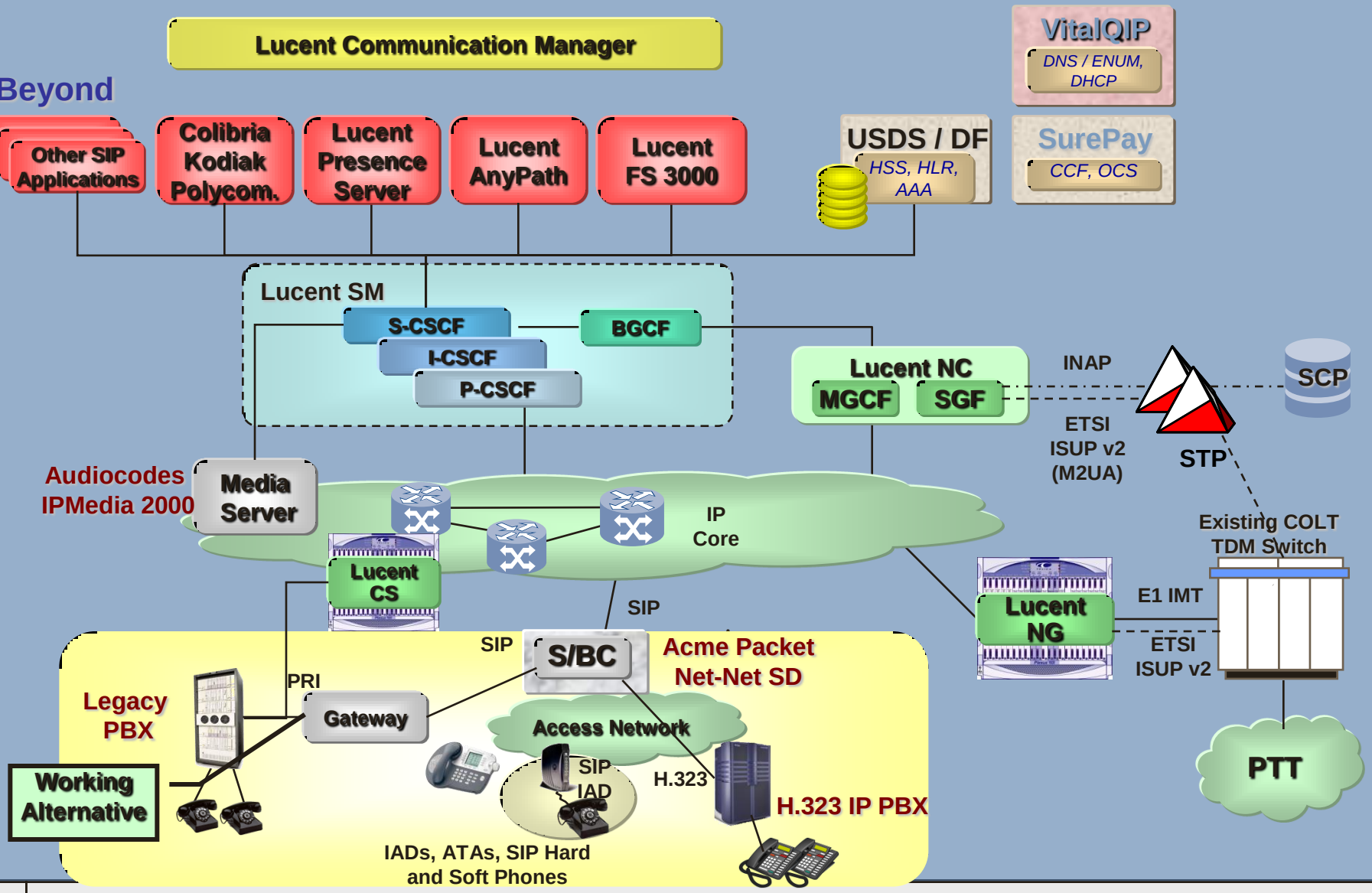
Ericsson


IMS control
SCP
HSS
IP Centrex
Broadband
telephony
Presence
Server
Feature
Server
Diameter
Access Gateway
Control Function (AGCF)
Media Gateway
Control Function (MGCF)
Feature
Server
Telephony
Softswitch
PSTN/ISDN
Emulation
Service
ISC
~SIP
SIP
CSCF
SIP
SIP
SIP
SIP
Telephony
Softswitch
RSS
V5.2
Q.931
EAR
TDM
H.248
(AGW)
IUA
H.248
MRFC
H.248
MRFP
ISUP
SIP/
H.323
H.248
PBX
TDM
MGW
MPLS/ IP
PBN Telephony
CCS
PSTN
MGW
RTP
RTP
RTP
MSAN
D
S
L
Broadband
access
Router/
BRAS
A-SBG
N-SBG
SIP/H.323
VoIP
IAD
SIP+RTP

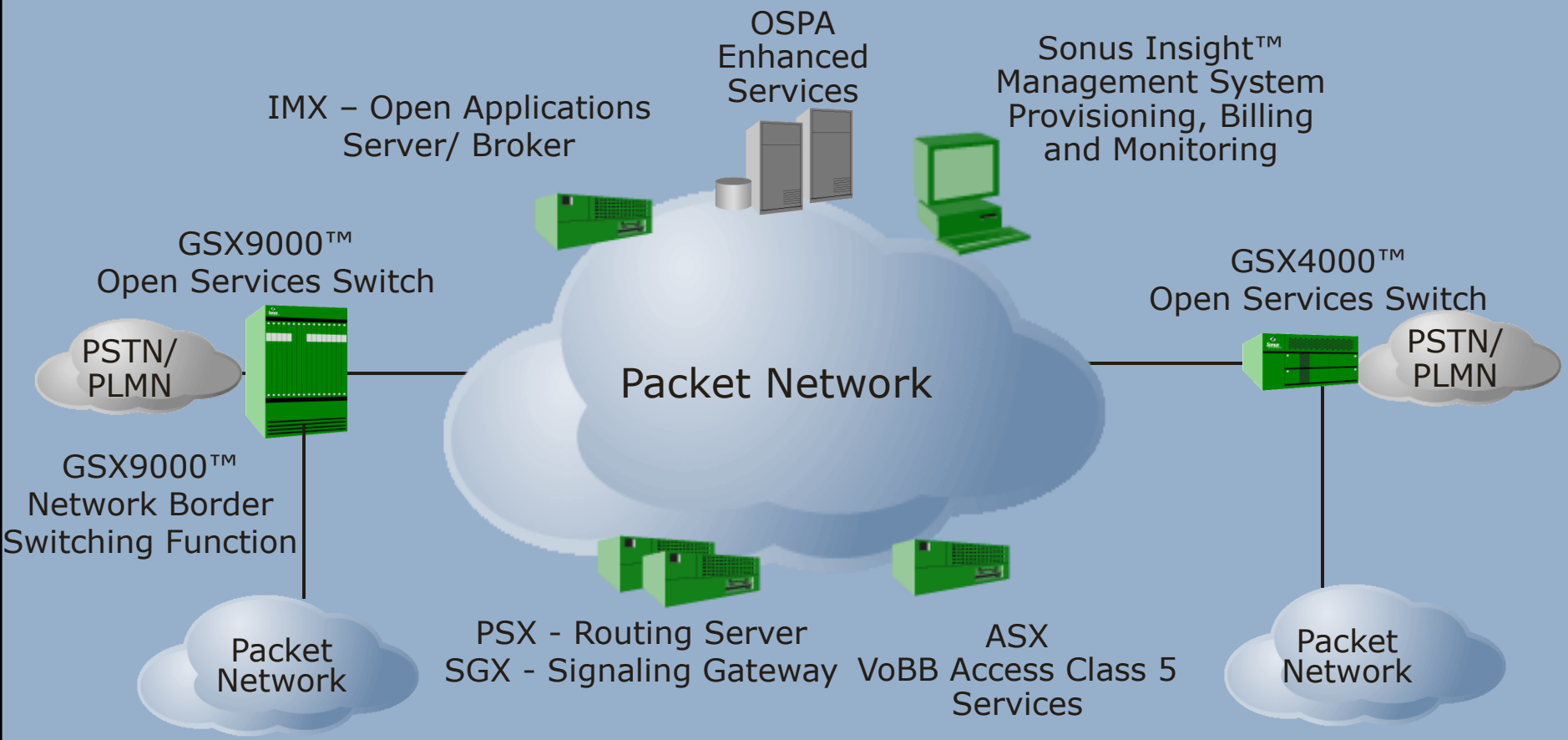
Cisco


Application Server
ISC
Presence Engine
HSS
Cx
Sh
CSCP-SE
PGW
ISUP
ISUP
MGCP
Billing & Measurement
COLT STP
COLT PSTN
MGW
SBC
FWSM
SIP-T
SIP
SIP
SIP
SIP
MGCP
MGCP
SIP/H.323 Interconnect Carrier
CSCP-EP
Reseller
SIP end-devices
SIP / H.323 IP PBX
COLT IP PBX
BRI PRI
BRI Q.SIG
PRI DPNSS
Carrier VoIP Service
COLT VoIP Reseller
COLT Voice Gateway
COLT IP-PBX
COLT Total
COLT Voice Integrate

Lucent


Lucent Communication Manager
Beyond
Other SIP Applications
Colibria Kodiak Polycom.
Lucent Presence Server
Lucent AnyPath
Lucent FS 3000
VitalQIP
DNS / ENUM, DHCP
USDS / DF
HSS, HLR, AAA
SurePay
CCF, OCS
Lucent SM
S-CSCF
I-CSCF
P-CSCF
BGCF
Lucent NC
MGCF
SGF
INAP
ETSI ISUP v2 (M2UA)
SCP
STP
Audiocodes IPMedia 2000
Media Server
IP Core
Lucent CS
SIP
Existing COLT TDM Switch
Lucent NG
E1 IMT
ETSI ISUP v2
SIP
S/BC
Acme Packet Net-Net SD
PRI
Legacy PBX
Gateway
Access Network
Working Alternative
SIP IAD
H.323
H.323 IP PBX
PTT
IADs, ATAs, SIP Hard and Soft Phones

Sonus


OSPA
Enhanced
Services
IMX – Open Applications
Server/ Broker
Sonus Insight™
Management System
Provisioning, Billing
and Monitoring
GSX9000™
Open Services Switch
GSX4000™
Open Services Switch
PSTN/
PLMN
PSTN/
PLMN
Packet Network
GSX9000™
Network Border
Switching Function
Packet
Network
PSX - Routing Server
SGX - Signaling Gateway
ASX
VoBB Access Class 5
Services
Packet
Network

VoIP Protocols

H.323

- ITU, ASN.1, CPE/Phone<->Gatekeeper
- H.225/RAS (1719/UDP) for registration
- H.225/Q.931 (1720/TCP) for call setup
- H.245 (>1024/TCP – or over call setup channel) for call management

MGCP (Media Gateway Control Protocol)

- IETF, Softswitch (CallAgent)<->MGW
- CallAgents->MGW (2427/UDP)
- MGW->CallAgents (2727/UDP)
- Used to control MGWs
- AoC (Advice Of Charge) towards CPE - **

VoIP Protocols

SIP

- IETF, HTTP-like
- Session based – Does anyone here not know what SIP is? :D

RTP

- Media stream (one or one per direction)
- CODECs (G.711{a,u}, G.726, G.729(a))
- RTCP: control protocol for RTP
- SRTP: Secure RTP (w/ MiKEY)
- Often 16000+/UDP or default NAT range, but can be any UDP>1024
- Can be UA<->UA aka “Free Intersite” or UA<->MGW<->UA

H.323 versus SIP

- The majority of current COLT VoIP products is based on H.323
  - This is mainly owing to missing functionality on SIP
  - Questionable interoperability and scalability concerns still exist though (10s of billions of minutes)
  - SIP not expected to completely replace H.323 in the mid/long term.
  - Protocols are somewhat complementary- no religion here though!
  - More detail on the differences
    - and more insight on understanding of our direction at:
    - http://www.packetizer.com/voip/h323_vs_sip/
    - This is expected to change over time

Session Border Controller

What the role of an SBC ?

- Security
- Hosted NAT traversal (correct signalling / IP header)
- Signalling conversion
- Media Conversion
- Stateful RTP pin-holing based on signalling

Can be located at different interfaces: Customer/Provider, inside customer LAN, Provider/Provider (VoIP peering)

What can be done on a FW with ALGs ?

What can be done on the end-system ?

Is there a need for a VoIP NIDS (especially with SIP-TLS)?

VoIP Hardware

Mix of software and hardware (mostly DSPs)

- Softswitch: usually only signalling
- MGW (Media Gateway): RTP<->TDM, SS7oIP<->SS7
- IP-PBX: Softswitch+MGW

Operating systems

- Real-time OSes (QNX/Neutrino, VxWorks, RTLinux)
- Windows
- Linux, Solaris

Poor OS hardening

Patch management:

- OSes not up-to-date
- Not “allowed” to patch them

Security Challenges

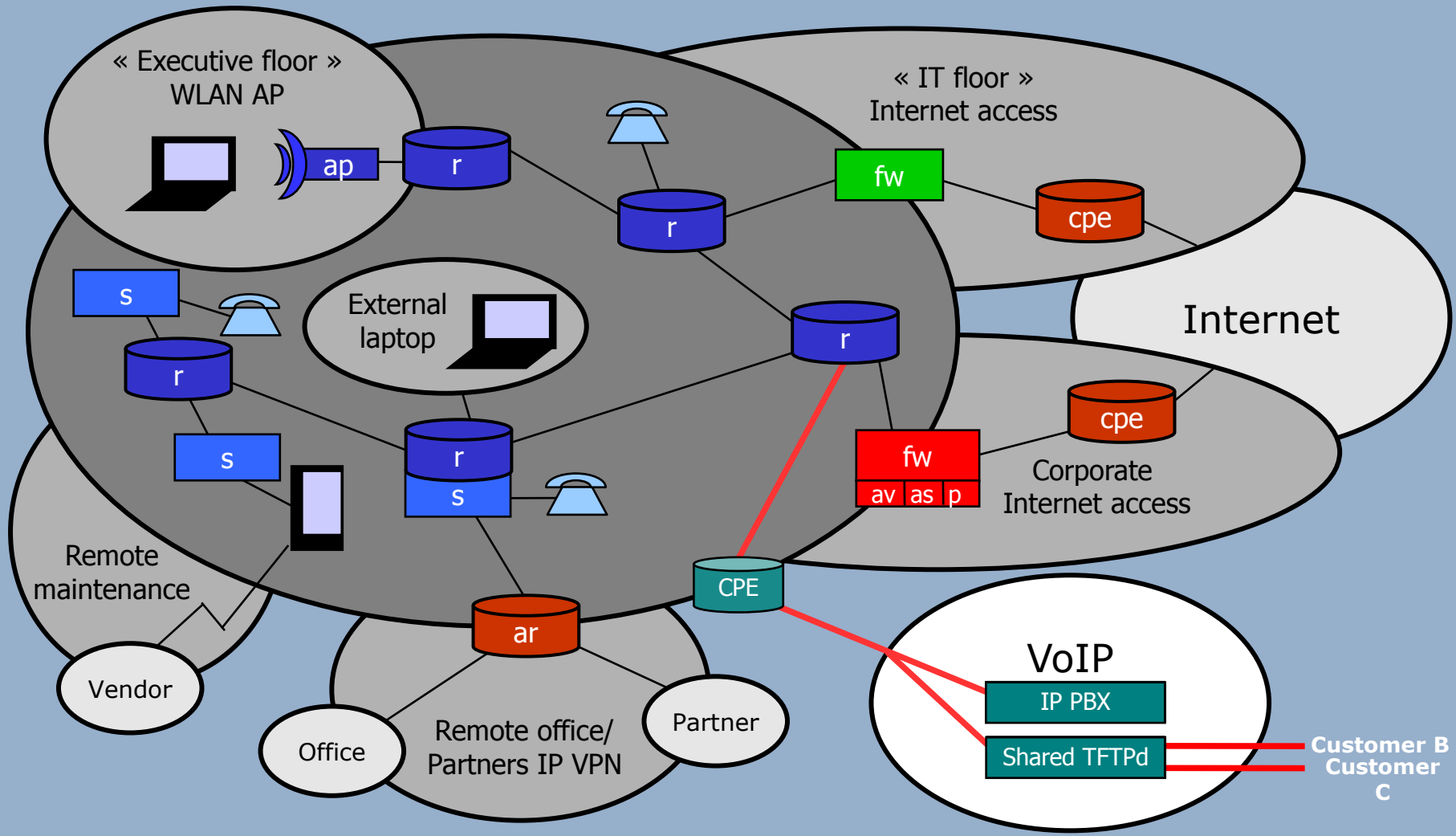
VoIP protocols

- No, VoIP isn't just SIP
- SIP is a driver for IMS services and cheap CPEs
- H.323 and MGCP (still) rock the carrier world

Security issues

- VoIP dialects
- Only a couple of OEM VoIP stacks (think x-vendor vulnerabilities)
- FWs / SBCs: do they solve issues or introduce complexity ?
- Are we creating backdoors into customer networks ?
- CPS and QoS

One more backdoor?



VoIP Dialects

No way to firewall / ACL (especially if non-stateful) based on protocol inspection

Vendors who never heard of timeouts and don't send keep-alives

Result :

- Clueful:
  - Permit UDP <port range> <identified systems>
- Half clueful:
  - Permit UDP <port>1024> any
- Clueless:
  - Permit UDP any any

End-result:

- 0wn3d via exposed UDP services on COTS systems
- Who needs RPC services (>1024/UDP) ?

Lawful Intercept

- Re-use existing solutions: TDM break-out
- Install a sniffer (signalling & media stream)
- Re-route calls (but hide it in the signalling)
- Eavesdropping not a real threat (own network)
- Enterprise network : Needs to be a part of a global security strategy – How many have this?
  - Clear text e-mail
  - Clear text protocols (HTTP, Telnet, etc)
  - VoIP
  - Etc
- VoIP over WLAN easy.

Phones and Terminals

IP Phones Reliability

- Quite easy to crash (weak TCP/IP stacks and buggy software implementation)
- Mostly an insider threat – How clueful is your cleaner?
  - DHCP server
  - TFTP server (phone configuration)
  - Credentials (login + PIN) – Fraud issues.

VoIP doesn't mean that you need to move to IP Phones

- PBX with E1 (PRI/BRI) to router and then VoIP
- PBX with IP interface towards the outside world (but do you really want to put your PBX on the Internet) ?
- Means that you have to maintain two separate networks, but "solves" the QoS issues on a LAN
- What about soft clients ?! – All the usual Unix/Windows issues.

Denial of Service

Generic DDoS

- Not a real issue, you can't talk to our VoIP Core
  - ACLs are complex to maintain use edge-only BGP blackholing
- We are used to deal with large DDoS attacks :)
  - http://www.securite.org/presentations/ddos/

DoS that are more of an issue

- Generated by customers: not too difficult to trace (IT Clue)
- Protocol layer DoS : H.323 / MGCP / SIP signalling
  - Replace CPE / use soft-client
  - Inject crap in the in-band signalling (MGCP commands, weird H.323 TPKTs, etc)
  - Get the state machine of the inspection engine either confused or in a block-state, if lucky for the "server" addresses and not the clients – Vendors not really thinking about this.

Security Challenges

Online services

- Call Management (operator console)
- IN routing (Fraud potential)
- Reporting / CDRs

Security issues

- Multi-tenant capabilities
- Have the vendors ever heard of web application security ?
- Who needs security or lawful intercept if a kid can route your voice traffic via SQL injection

WebApp FWs are really required...

Security Challenges

TDM / VoIP : two worlds, two realms, becoming one ?

- Security by “obscurity” / complexity vs the IP world
- Fraud detection

Security issues

- New attack surface for legacy TDM/PSTN networks
- No security features in old Class4/Class5 equipment
- No forensics capabilities, no mapping to physical line
- Spoofing and forging
- People: Voice Engineers vs Data Engineers vs Security engineers. Engineering vs Operations. Marketing vs Engineering. Conflicts and Time-to-Market

Operational Concerns

VoIP is damn complex

Only way to debug most of the issues: VoiceEng + IP/DataEng + SecurityEng on a bridge/online chat

Requirement: be able to sniff all traffic

Tool: Ethereal/Wireshark

Attacker: Just use any of the protocol decoder flaw in the sniffer

Make sure your sniffers are on R/O SPAN ports, in a DMZ which only allows in-bound VNC/SSH

Do not underestimate the effort on a multi Country setup – What is EU?!

If the guy is really good and can upload a rootkit over RTP: get his CV and offer him a job – you need this guy – serious skills shortage

VoIP Carrier Interconnect

Aka “VoIP peering” / Carrier interconnect

Already in place (TDM connectivity for VoIP carriers/Skype{In, Out})

Connectivity: over the Internet, IX (public/private), MPLS VPN or VPLS (Ethernet)

No end-to-end MPLS VPN, break the VPN and use an IP-IP interface

Hide your infrastructure (topology hiding), use {white, black}listing and make sure only the other carrier can talk to you

Signalling/Media conversion (SBC)

Remember – this isn’t web traffic – its termination money in both directions!

Encryption / Authentication

Do we want to introduce it ?

Vendor X: “We are compliant”. Sure.

Vendor Y: “It's on our roadmap”. Q1Y31337 ?

Vendor Z: “Why do you need this ?”. Hmmmm...

IPsec from CPE to VoIP core

> Doable (recent HW with CPU or crypto card)

> What about CPE<->CPE RTP ?

> Still within RTT / echo-cancellation window

May actually do mobile device<- IPsec ->VoIP core

> Bad guys can only attack the VPN concentrators

> No impact on directly connected customers

Still reliability issues in vendor implementations

IMS Security – The Future

IMS = IP Multimedia Subsystem

Remember when the mobile operators built their WAP and 3G networks ?

- Mostly “open” (aka terminal is trusted)
- Even connected with their “internal”/IT network

IMS services with MVNOs, 3G/4G: overly complex architecture with tons of interfaces

Large attack surface: registration/tracking servers, application servers, etc

Firewalling: complex if not impossible

Next thing to try: Attack Fixed<->Mobile handover (GSM<->WiFi)

Questions?