WiMAX
GTER 19

Luiz Eduardo Dos Santos
CISSP, CWSP, CWAP
Principal Network & Security Engineer

ARUBA

Glossary

BS – base station

SS – subscriber station

AAS – Adaptive Antenna System

MiMo – multiple input/ multiple output

Service Profile

BWA - Broadband Wireless Access

FEC – Forward Error Correction

ARQ – Automatic Repeat Request

FDD – Frequency Division Duplexing

TDD – Time Division Duplexing

UL and DL – uplink and downlink

RLC – Radio Link Control

What is WiMAX?

Complements 802.11

IEEE 802.16 (started in 2001)

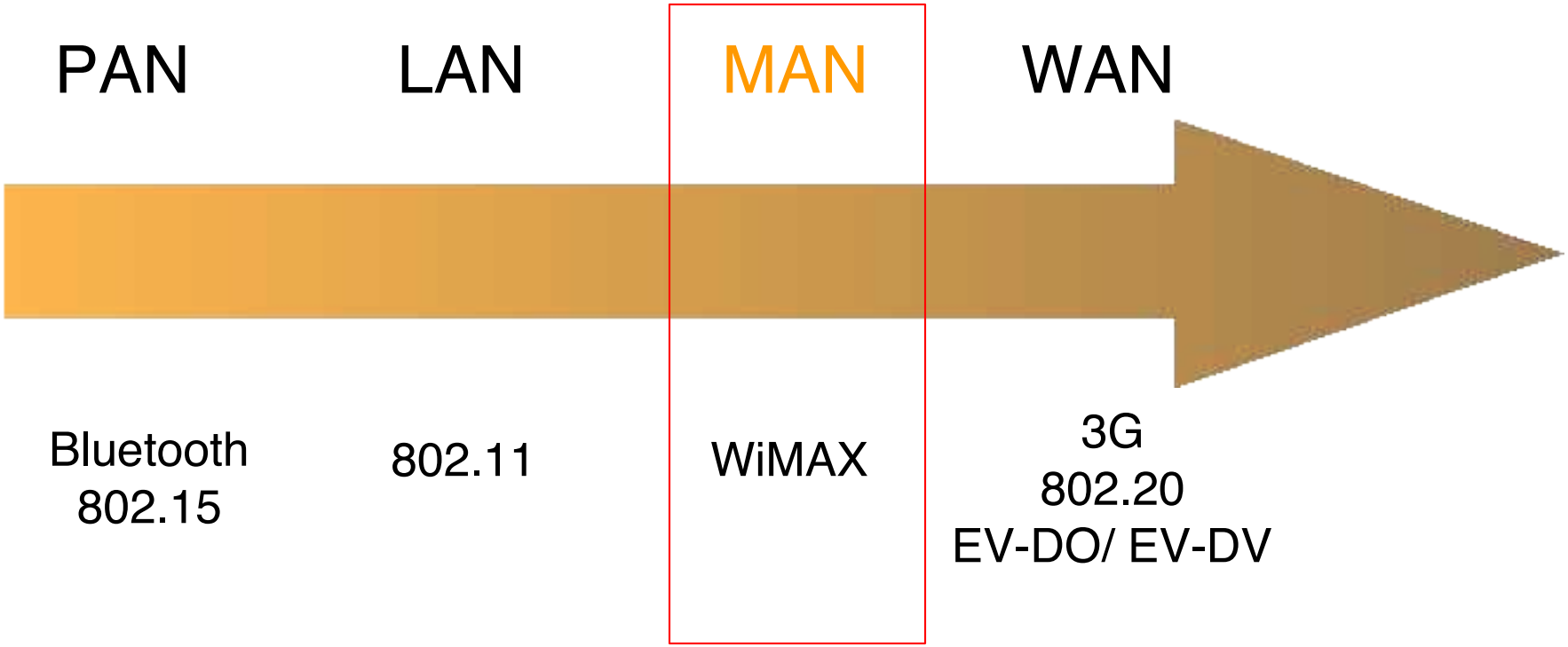
2-66 Ghz* (licensed and non-licensed bands)

Worldwide Interoperability for MicroWave Access

Typically up to 20km (couple mpbs in 50km)

Typically up to 48Mbps (75Mbps best case scenario)

Where does it fit?



802.16 Standards

802.16.1 - 10-66 GHz, line-of-sight, up to 134Mbit/s

802.16.2 - minimizing interference between coexisting WMANs.

802.16a - 2-11 Ghz, Mesh, non-line-of-sigth (2003)

802.16b - 5-6 Ghz

802.16c - detailed system profiles

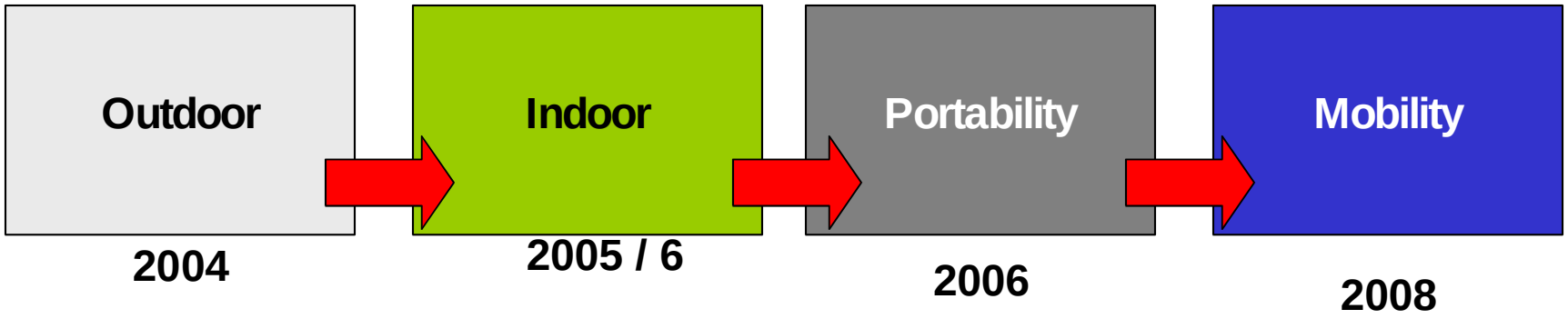
802.16d – consolidates 802.16 a and 802.16c / indoor CPE (NLOS) and OFDM sub-channeling

802.16e - Mobile Wireless MAN

802.16f – Multihop functionality

802.16g – addresses efficient handover and improves QoS support

WiMAX evolution



What WiMAX is

Standard BWA technology

Interoperability

Convenience of NLOS (802.16a)

Hotspot wireless backhauling

BWA for places without existing broadband

QoS built into MAC

Variants

WirelessMAN – SC	PTP	LOS	10-66Ghz	TDD & FDD
WirelessMAN-SCa	PTP	NLOS	2-11Ghz	TDD & FDD
WirelessMAN-OFDM (256-point transform)	PTMP	NLOS	2-11Ghz	TDD & FDD
WirelessMAN-OFDMA (2048-point transform)	PTMP	NLOS	2-11Ghz	TDD & FDD
WirelessHUMAN (Highspeed Unlicensed Metro Area Network)	PTMP	NLOS	2-11Ghz	TDD

WiMAX promises

Full Mobility with 802.16e

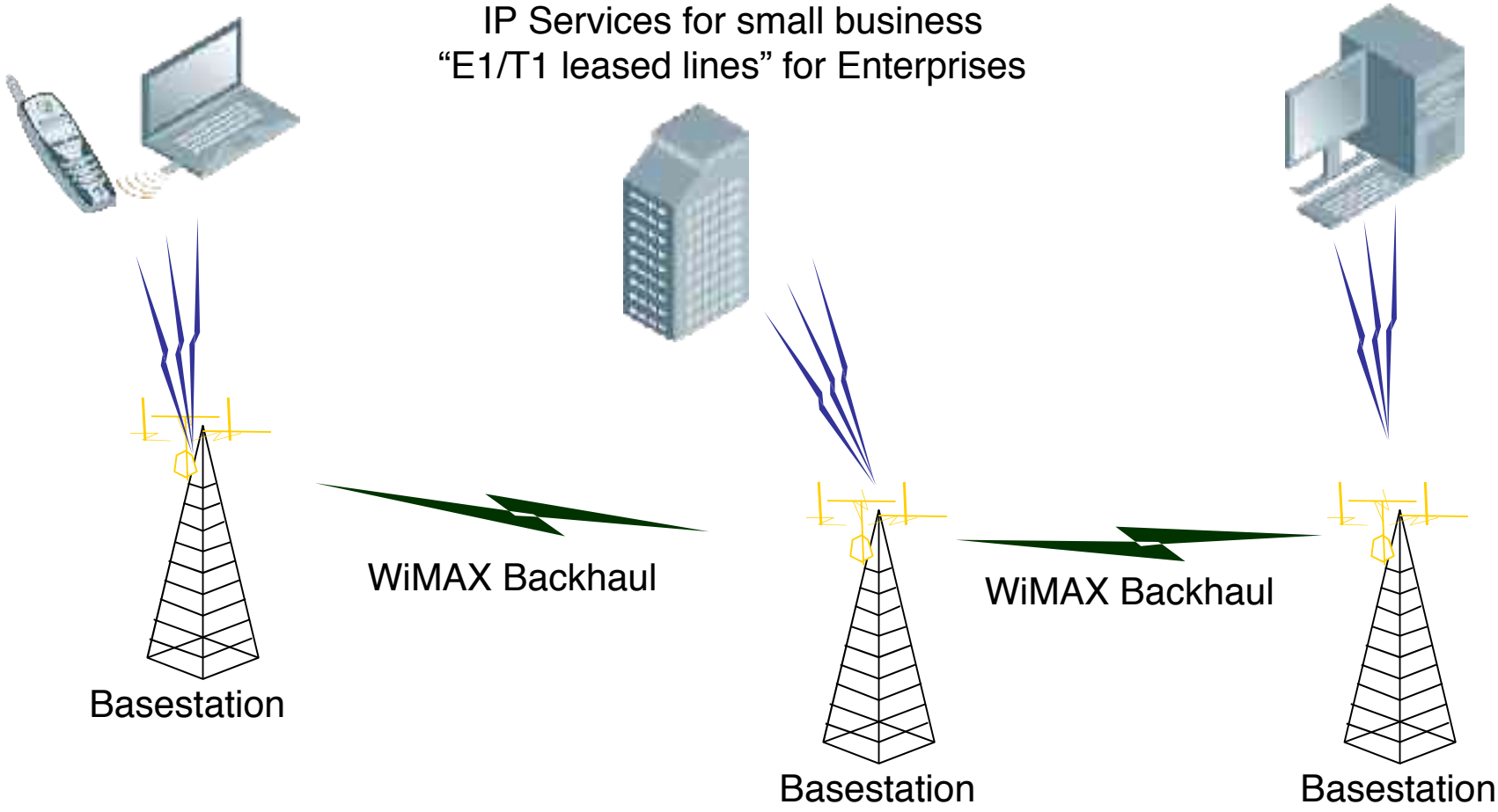
Targets the replacement of landlines, enabling voice over WiMAX

Applications

802.16e

802.16a
Wireless backhaul for WiFi hotspots
IP Services for small business
“E1/T1 leased lines” for Enterprises

Residential/ “Wireless DSL”



PHY & MAC

MAC CONVERGENCE SUBLAYER (ethernet, IP, etc)
MAC LAYER (arq, QoS, fragmentation and packing)
MAC PRIVACY SUBLAYER (authentication, key-exchange, encryption)
PHYSICAL LAYER (OFDM, power level control, tx, rx, ranging)

Service Class & QoS

Unsolicited Grant Services (UGS): CBR services

Real-Time Polling Services: variable size data packets (i.e. VoIP w/ silence suppresion)

Non-Real-Time Polling Services: non-real-time services

Best Effort: others, internet data, etc.

QoS

Legacy and WiMAX-specific methods to create and maintain service flows

Bandwith requests and grants

- GPC – grant per connection
- GPSS – grant per SS

Types of service

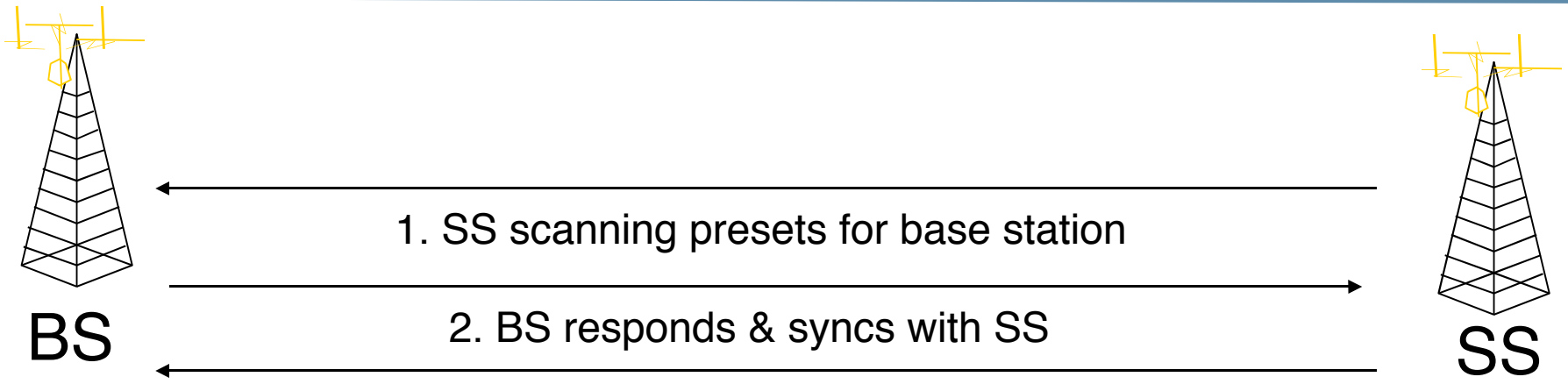
- UGS (Unsolicited Grant Services)
- Realtime Polling Services
- Non-realtime Polling Services
- Best Effort

Security

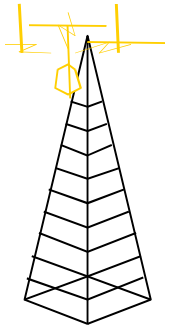
Authentication: Privacy Key Management (PKM) protocol to provide distribution of keying data via x.509 digital certificate and RSA public/private key

Encryption (DES in CBC mode): done at the MAC privacy sublayer ,encapsulation protocol, applied to MAC PDU payload.

How does it work?



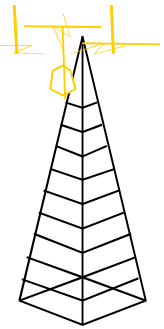
How does it work? (Cont)



BS

1. SS sends auth request with authentication info (X.509 cert)

2. BS sends auth reply, with auth key encrypted with SS's public key



SS

3. With success auth, SS registers with network and gets ip via DHCP and gets ip address of TFTP server to get its config

4. BS accepts SS and is ready for service flow

ARUBA

Mesh Topology

No centralized BS

Each node serves as both AP and wireless router

Multiple pathways to the wireless signal

Requires specialized client software that will provide the routing function and put the radio into ad-hoc or infrastructure mode

What else in the wireless world?

MiMo

EV-DO / EV-DV

802.11n

Capwap/ LWAPP

802.20

(my) Conclusion

Expected same fuzz as 802.11 in a couple of years

Portability first, mobility later when 802.16e laptop chips are ready (10 Mbps < 2km)

We'll hear the term "WiMAX-ready" for a while

Great technology for wireless MAN, addressing multipath, interference and mobility (instead of portability) in the future

Obrigado!

luiz (at) arubanetworks.com