WiMAX

Clemens H. Cap

http://wwwiuk.informatik.uni-rostock.de

http://www.internet-prof.de

http://www.wimax-prof.de

For those believing in acronyms

The basic idea

Wireless Microwave Access

Wireless Metropolitan Access

The wireless backbone / MAN

Think of it as Wi-Fi on steroids. **Business Week**

For the pedestrian

Application Modes

In WLAN

- Access Point
- Ad Hoc
- Wireless Distribution / Mesh

In WiMAX

Basestation	**Standard**	WiMAX way of life	802.16
Mesh	**Optional**	WiMAX way of life	802.16a
Mobile	**Future**	WiMAX way of life	802.16e

WLAN Application Mode
Access Point

Client

Access Point

Client

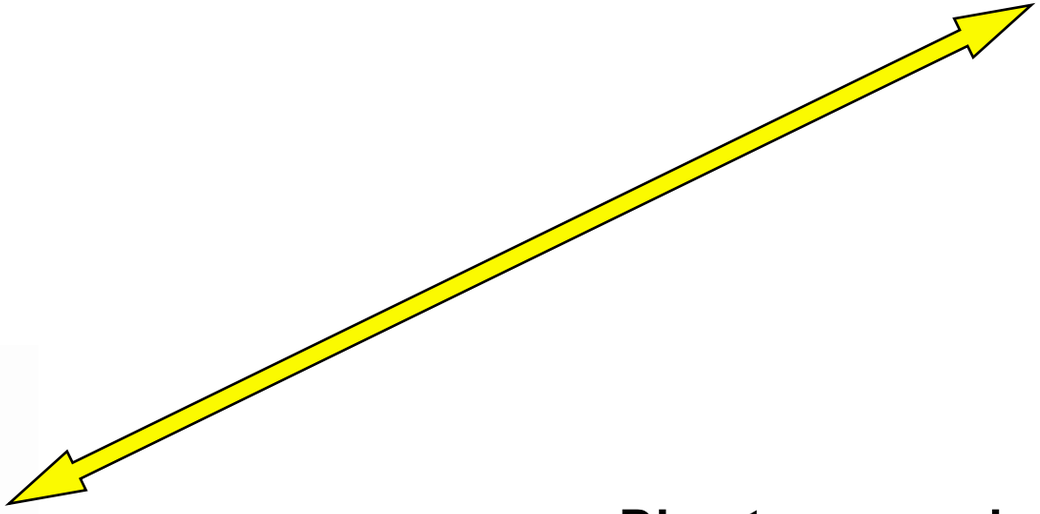
Client

All communication uses AP
AP may serve as bridge to wired world
AP may serve as firewall
May use different channels

WLAN Application Mode
Ad Hoc

Client

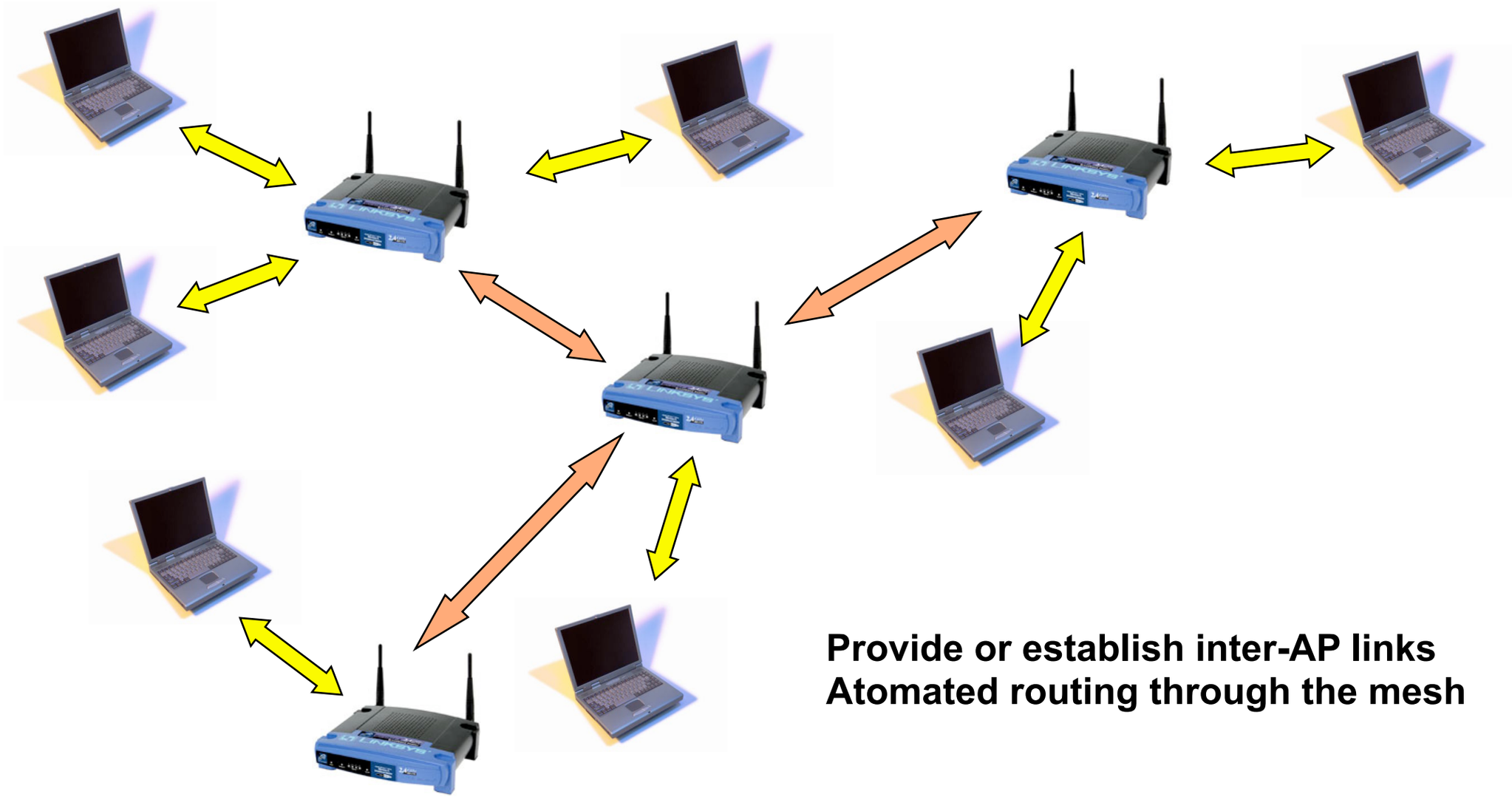
Client



Client

Direct communication
Must use same channel

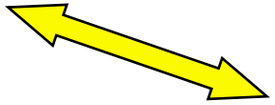
WLAN Application Mode
Wireless Distribution System / Mesh

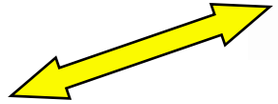


Provide or establish inter-AP links
Atomated routing through the mesh

WiMAX Application Mode
Basestation

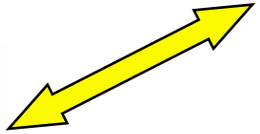
Subscriber Station





Subscriber Station

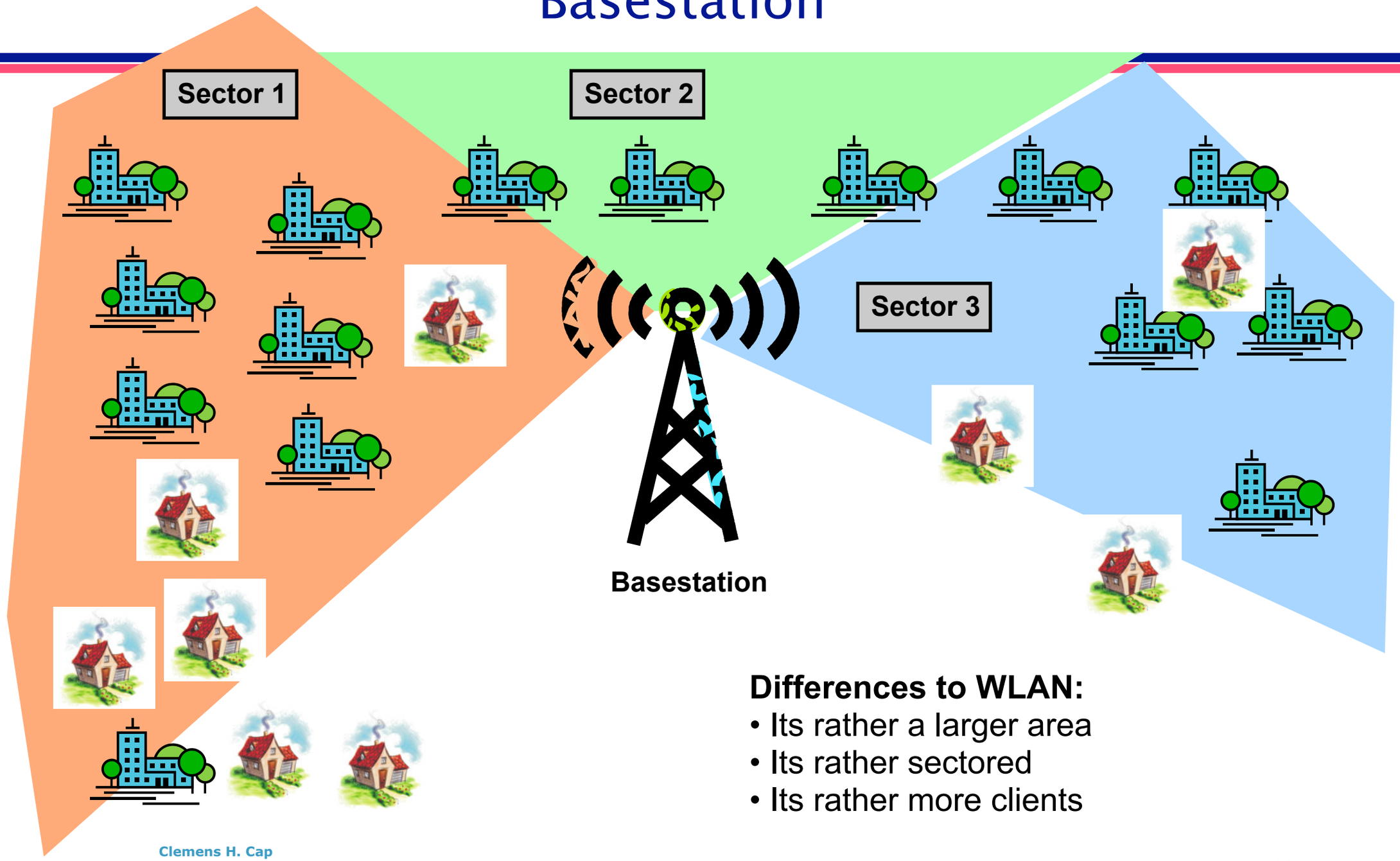
Basestation



Subscriber Station

All communication uses BS
BS may serve as bridge to wired world
Very similar to access point mode

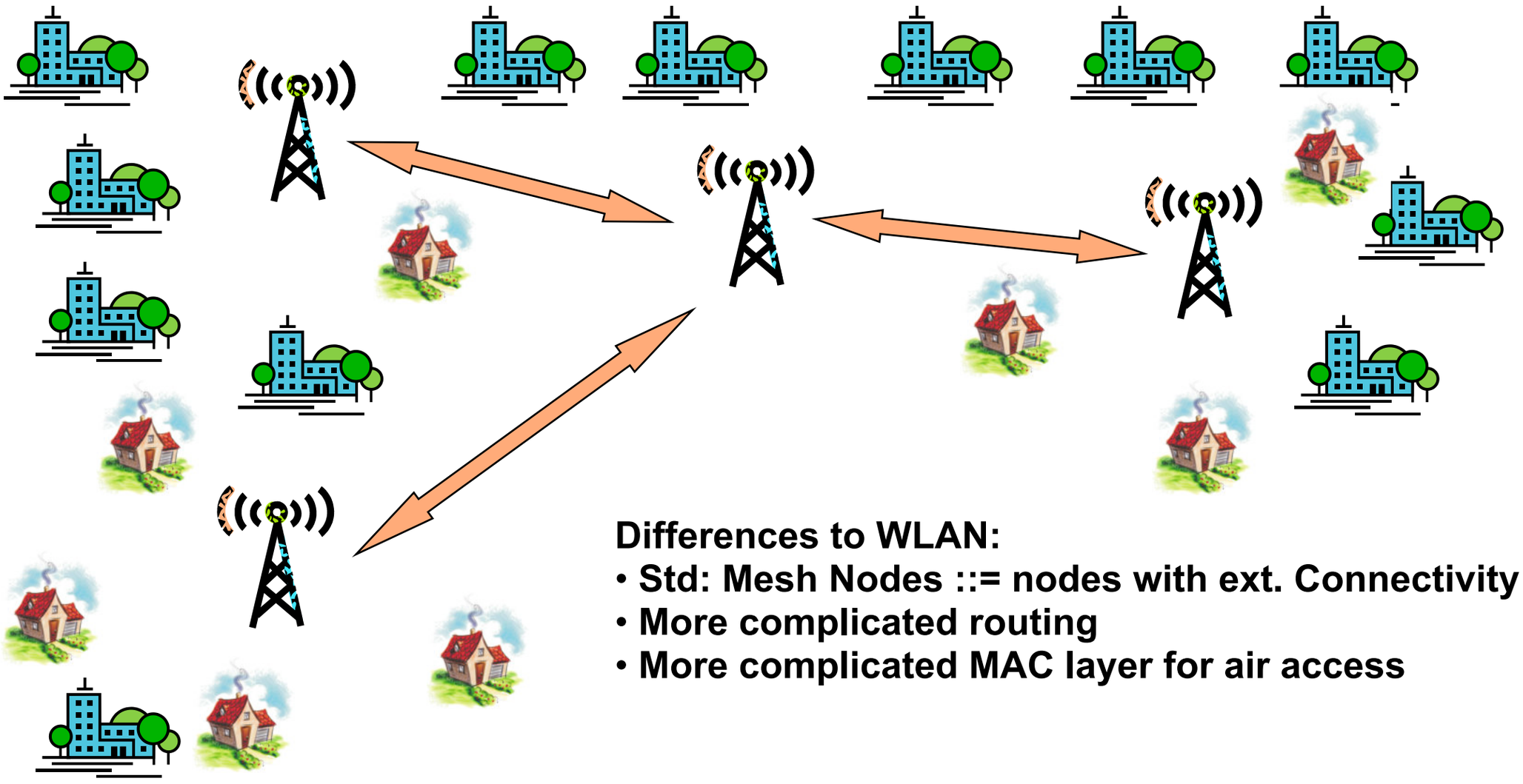
WiMAX Application Mode Basestation



Differences to WLAN:

- Its rather a larger area
- Its rather sectored
- Its rather more clients

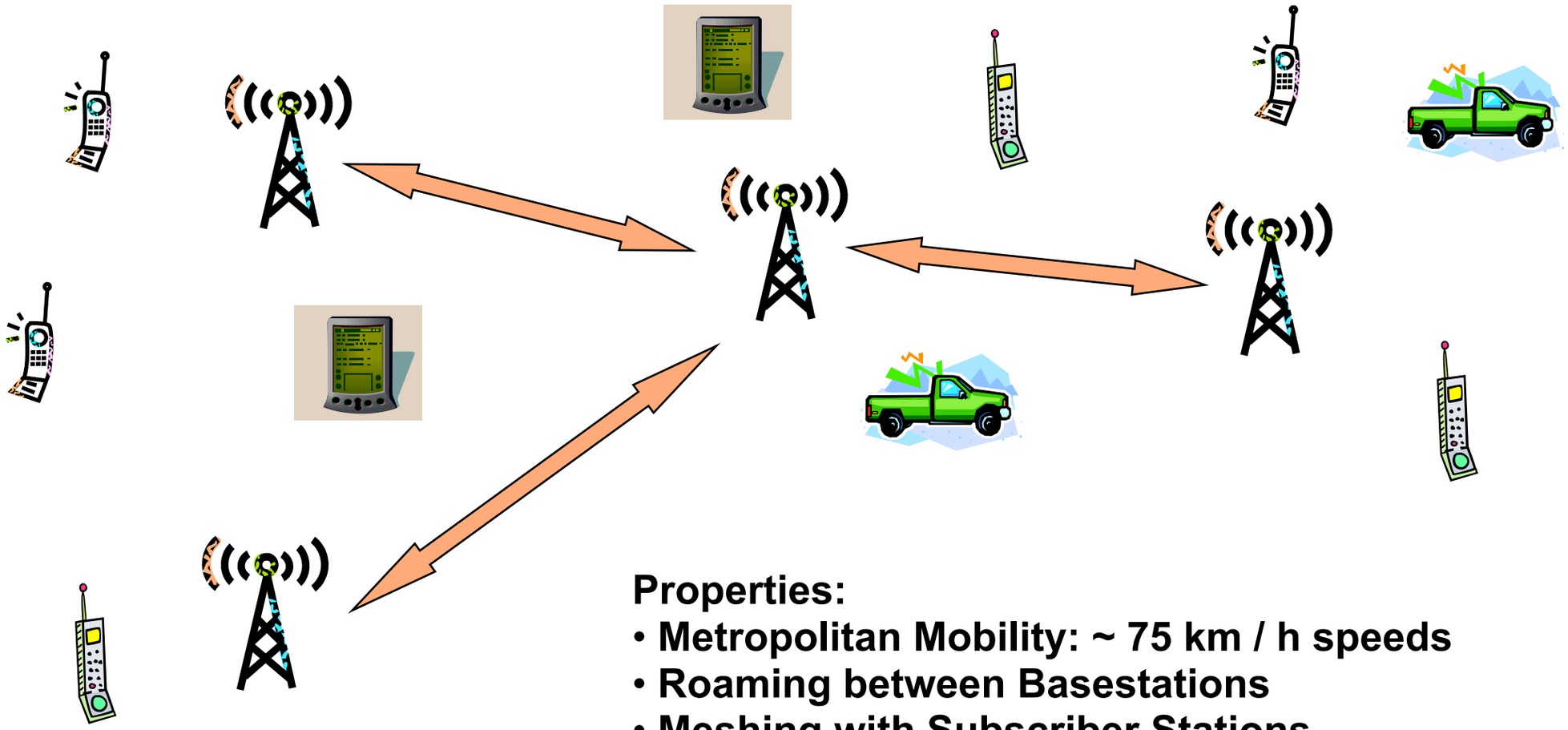
WiMAX Application Mode
Mesh



Differences to WLAN:

- **Std: Mesh Nodes ::= nodes with ext. Connectivity**
- **More complicated routing**
- **More complicated MAC layer for air access**

WiMAX Application Mode
Mobile



Properties:

- **Metropolitan Mobility: ~ 75 km / h speeds**
- **Roaming between Basestations**
- **Meshing with Subscriber Stations**

Application Areas (1)

Broadband Access: **T1 / E1 and better, but without wires, for high end users**

- Outdoor antenna on the roof, Clear Line of Sight
- Stationary application
- Basestation to Subscriber Station Traffic

802.16

Wireless Last Mile: **Yet another consumer last mile solution**

- Sold as W-DSL in combination with WLAN
- Also: Dropping WLAN, WiMAX to the home user
- Indoor antenna, Non Line of Sight
- Meshing

802.16a

Mobile Universal Serv.: Yet another mobile comm (phone) solution

- Competition for UMTS
- Roaming

802.16e

Application Areas (2)

Dedicated radio link: Standardized technology for a classical problem

Developing Countries: Entry technology into high speed communications

- Low cost equipment, no infrastructure required
- „Low barrier“ technology

Emergency, Security and Surveillance

- Easy, quick field deployment
- Bandwidth for video surveillance possible
- (Good ?) encryption included
- Does not require infrastructure operator
  - á closed circuit operations possible
  - á low cost (only the equipment)

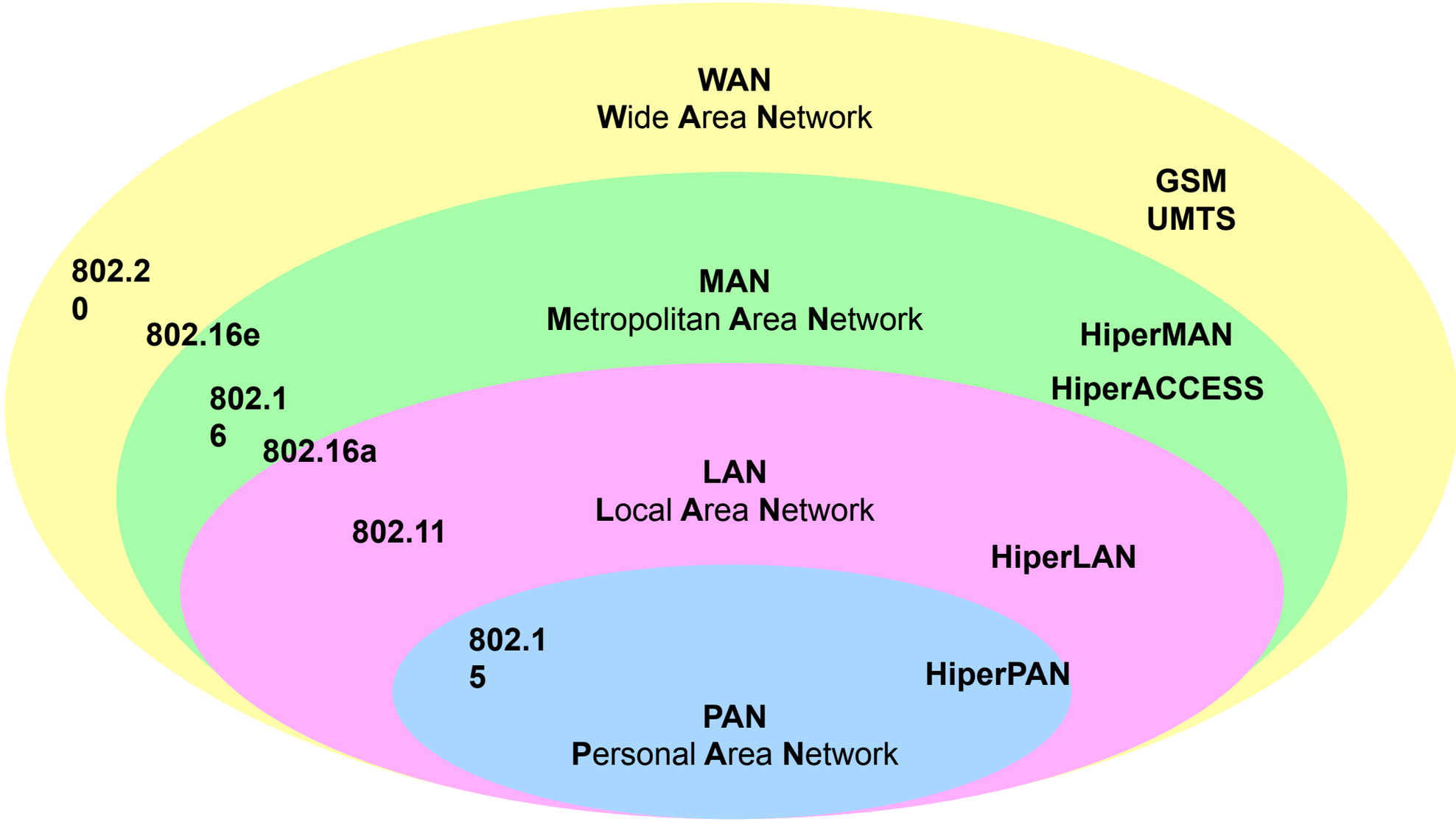
Big Brother !

Factors for Application Areas

Area	Scale ability	Performance	Cost	Standard	Interoperable
Broadband Access	+	+++	++	+	++
Wireless Last Mile	++	+	+++	+	+++
Mobile Universal Service	++	+++	+	+++	+++
Dedicated Radio Link	+	+++	+++	+	0
Developing Countries	+	++	+++	++	+
Emergency, Security and Surveillance	+++	+++	+++	0	0

For the standards people

The families



Standardization Activities (1)

802.16	Original standard 10 - 66 GHz Line of sight, Point to point
802.16a	Extension to 2-11 GHz Non line of sight, Point to multipoint
802.16REVd	Merger of 802.16 and 802.16a Errata andSystem Profiles
802.16e	Extension for mobility for vehicular speeds Extension for roaming
802.16c	Amendment for 10-66 GHz system profiles
802.21	Media independent handoff (802.3, 802.15, 802.11, 802.16)
802.20	Mobile Broadband Wireless Access MBWA » Compares to 802.16e » Looks at high speed mobile user up to 250 km / h » Standardization lagging behing 802.16

Certification (1)

Problem: **IEEE 802.16 is yet another flawed standard**

- Very broad and occasionally vague
- Outlines messages and possibilities
- Lacks algorithms, procedures, clear implementation guarantees
- Does not define compliance tests
- **Will not automatically lead to interoperable systems**

WiMAX Forum: Goal is „to ensure compatibility and inter operability“

- **Trademark** „WiMAX Forum™ Certified“
- **Different** from non protected „WiMAX Compliant“
- **Certification Work Group** defines interoperability standards & procedures
- More than 230 members (as of Q1 2005)
- Quarterly growth rate of more than 40%

Certification (2)

Certification Process of Wimax Forum

- First „WiMAX Forum™ Certified“ systems available in Q1 2005
- Ensure interoperability with ETSI HiperMAN standards
- Cetecom Lab in Spain selected as certification lab
- Revised target date for first certification: July 2005

Process

- Forum defines PICS (Protocol Implementation Conformance Statements)
- Forum defines Test Suites
- Lab conducts the tests

For the architecture and technical people

The three 802.16 Standards

802.16	802.16a	802.16e
Line of Sight	Near Line of Sight	Near Line of Sight
10 – 66 GHz	2 – 11 GHz	2 – 6 GHz
32 – 134 Mbps	75 Mbps	15 Mbps
1 – 3 miles	3 – 5 miles, max 30 miles	1 – 3 miles
Fixed	Fixed	Metropolitan Mobility Roaming

Compared to 802.11 (1)

Criterion	802.11	802.16
Range	**Very small** Optimized for 100 m	**Considerably larger** Optimized for 7 – 10 km Up to 50 km range
Indoor vs Outdoor	**Preferably Indoor** PHY tolerates only low multi-path delay spreads	**Indoor (16a) Outdoor (16, 16e)** PHY tolerates high multi-path delay spread (10 µsec = 3 km) Trees, buildings, persons
Scalability	**Poor** Fixed bandwidth of 20 MHz Fixed channels Certain degree of channel overlap	**Excellent** Variable bandwidth 1.5 MHz – 20 MHz Only limit is available spectrum
Licensing	**Unlicensed bands**	**Licensed and unlicensed bands**
Bandwidth	**Low to medium** 1 Mbps - 11 Mbps - 54 Mbps - 108 Mbps Efficiency 2,7 bps / Hz peak	**High** 75 - 100 Mbps – 134 Mbps Efficiency 5 bps / Hz

Compared to 802.11 (2)

Criterion	802.11	802.16
MAC Layer	**Contention based MAC: CSMA / CA**	**Grant based MAC**
Security	**Mostly questionable** **Various attempts on improvements** WEP, WPA	**Supposedly good** **Nevertheless flawed in principle** 3DES, AES
QoS	**No QoS** 802.11e upcoming	**Good QoS** 4 QoS classes for voice & video

Layer Architecture

User

Specific Service Access Point

MAC Convergence Layer

ATM
Ethernet, VLAN
PPP
IPv4, IPv6

MAC Service Access Point

Main MAC Layer

Framing
Slot Reservation
Fragmentation & Packing
Retransmission (ARQ)
Quality of Service (QoS)

Security (Standard: Privacy) Layer

Authentication
Key Exchange and Re-Keying
Encryption

PHY Service Access Point

Physical Layer

Modulation
Channel and frequency selection
Power Control
Transmit & Receive

Layer Architecture Observations

User will always use a convergence layer

- In a nutshell: Using Wimax is programming IP sockets

Security is a seperate layer

- Recognized by its own right, which is good when compared to 802.11
- Is placed just above the PHY, which is a good place for encapsulation
- But: It has a number of flaws
- One of the problems: Many management messages are not encrypted

Profiles

- For every layer there are several variants defined by profiles
- 5 PHY variants
- 2 MAC variants

Layer Architecture
Existing Profiles

MAC

- Point-to-Multipoint
- Meshing

What we expect them to be
From the introduction to this talk

PHY

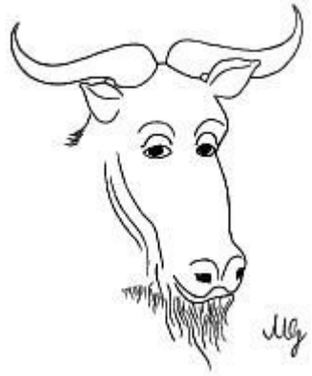
- WirelessMAN-SC
- WirelessMAN-SCa
- WirelessMAN-OFDM
- WirelessMAN-OFDMA
- WIrelessHuman

Quite a number of intriguing
Differences regarding supported features

For the
open networkers
community networkers

Open Source

Linux: **We are doing our own operating system**
Gcc: **We are doing out own compiler**
Wiki: **We are doing our own content**
WikiNews: **We are doing our own news**



CopyLeft:

- Everyone has access to the state of the art
- Everyone can contribute, add and modify
- Own contribution, if distributed, is again „CopyLeft“

Effect:

- We all participate for our common benefit
- Everyone can participate on identical conditions
- Noone can monopolize or block development

Sufficient proof that it can be done

And it can be done successfully

Open Net

OpenNet: **We are doing our network**

Idea:

- **Every terminal node also is routing node**
- **Every additional consumer device builds upon the infrastructure**
- **Let us assume a sufficient density of nodes**

- **Result:**
- **We have a working network – without a provider**
- **We are structurally autonomous**
- **No bit-tax, no pay-per-use (but no space for illegal stuff as well !)**

OpenNet and ClosedNet compared

- The net belongs to the provider / carrier
- The net belongs to its users

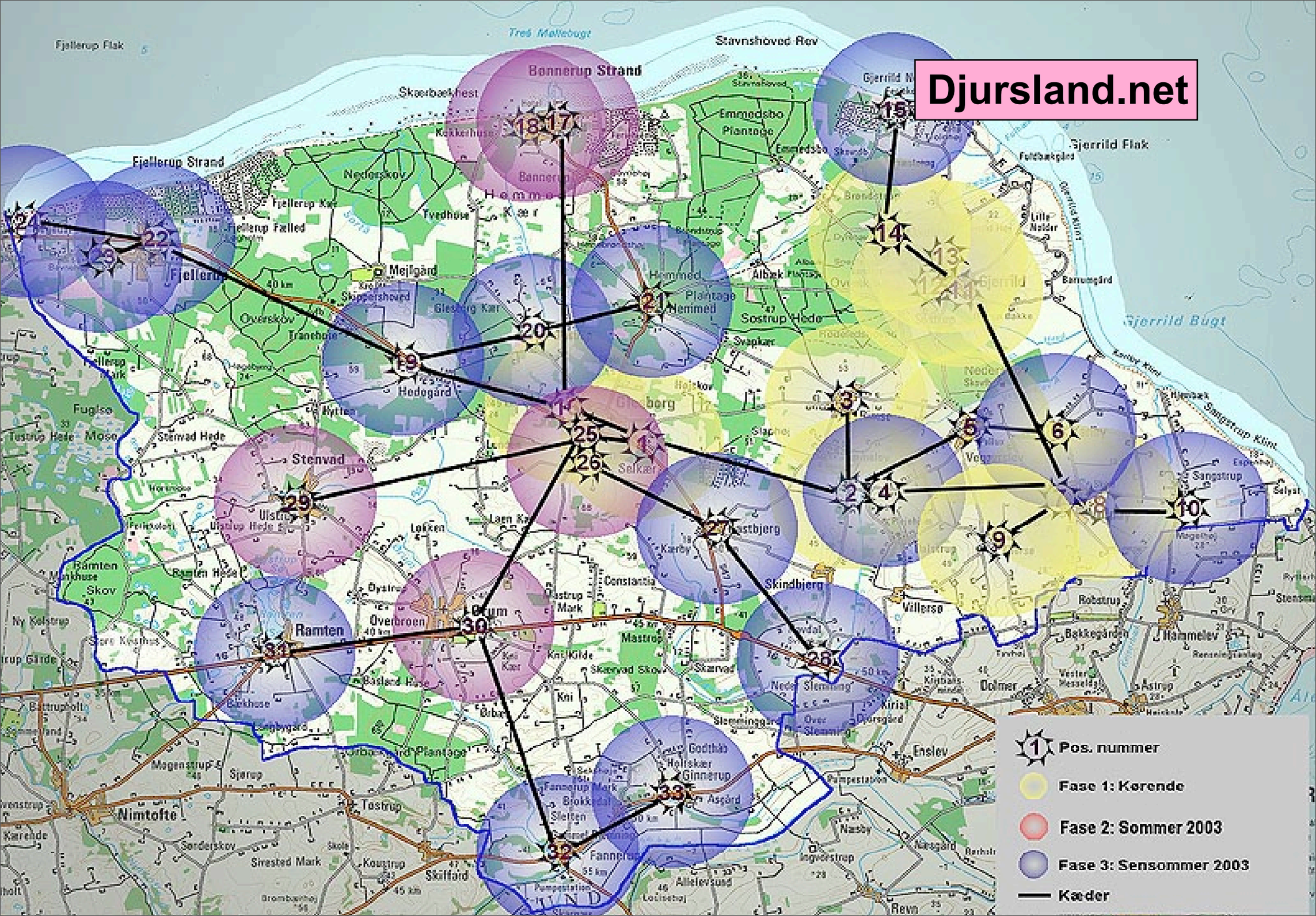
- Monopolists and investors which must be regulated and watched carefully
- No monopolists, no investors, no market dominance

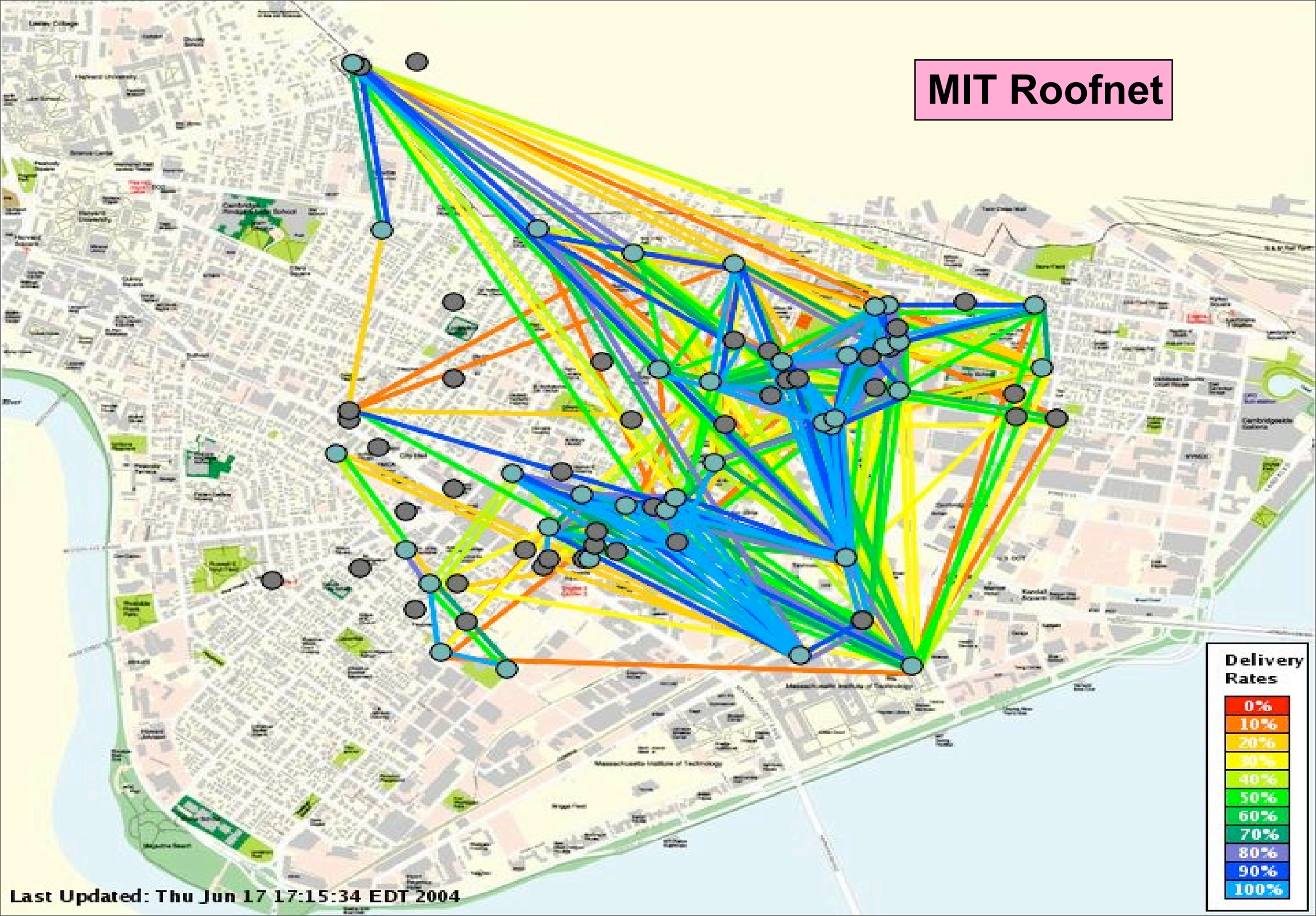
- Commercial profiling of users, big brother is watching us, data harvesting on citizen
- No centralized provider, less chance for big brother

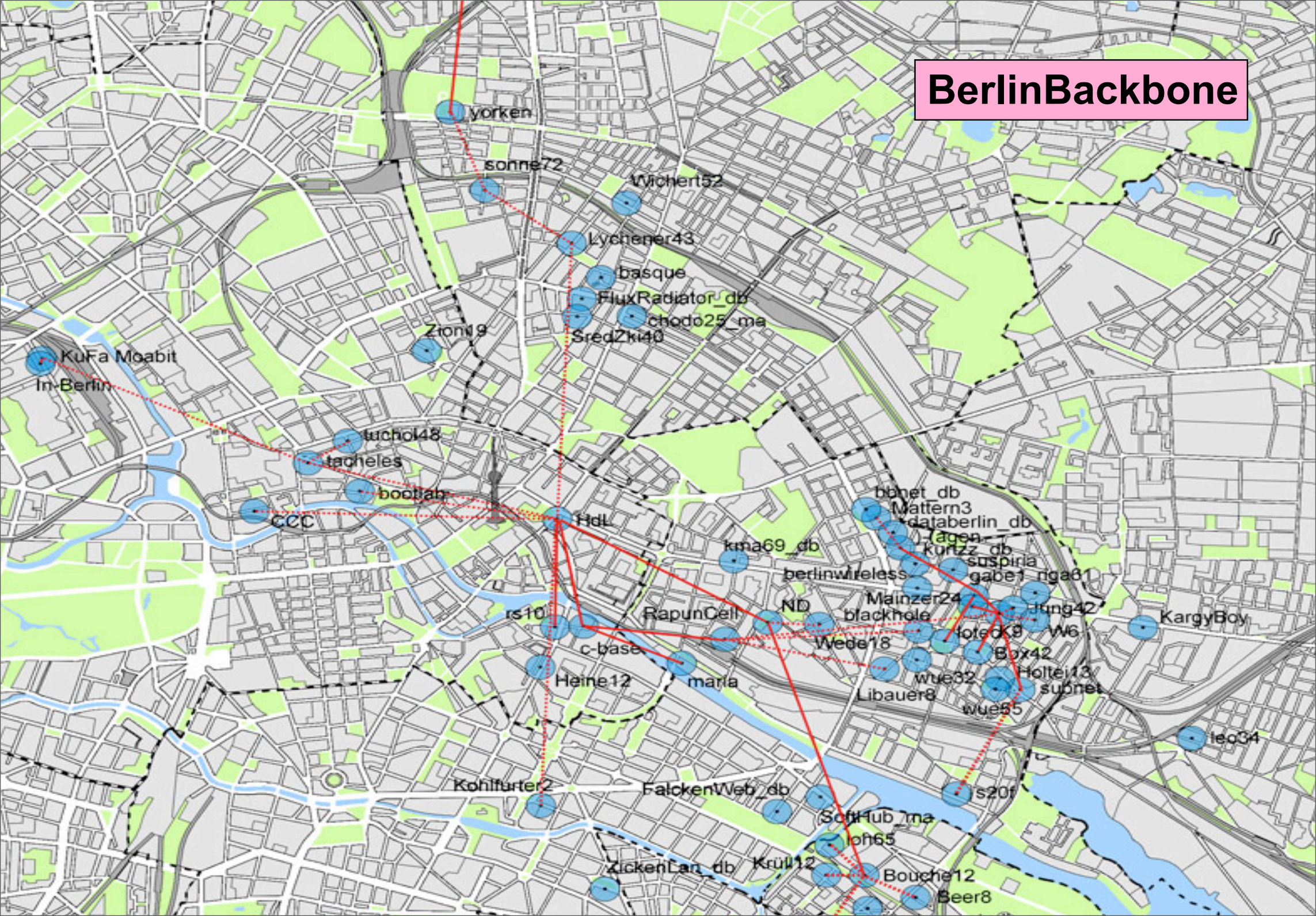
- Return on investment for the investor
- Creating and using value by the user

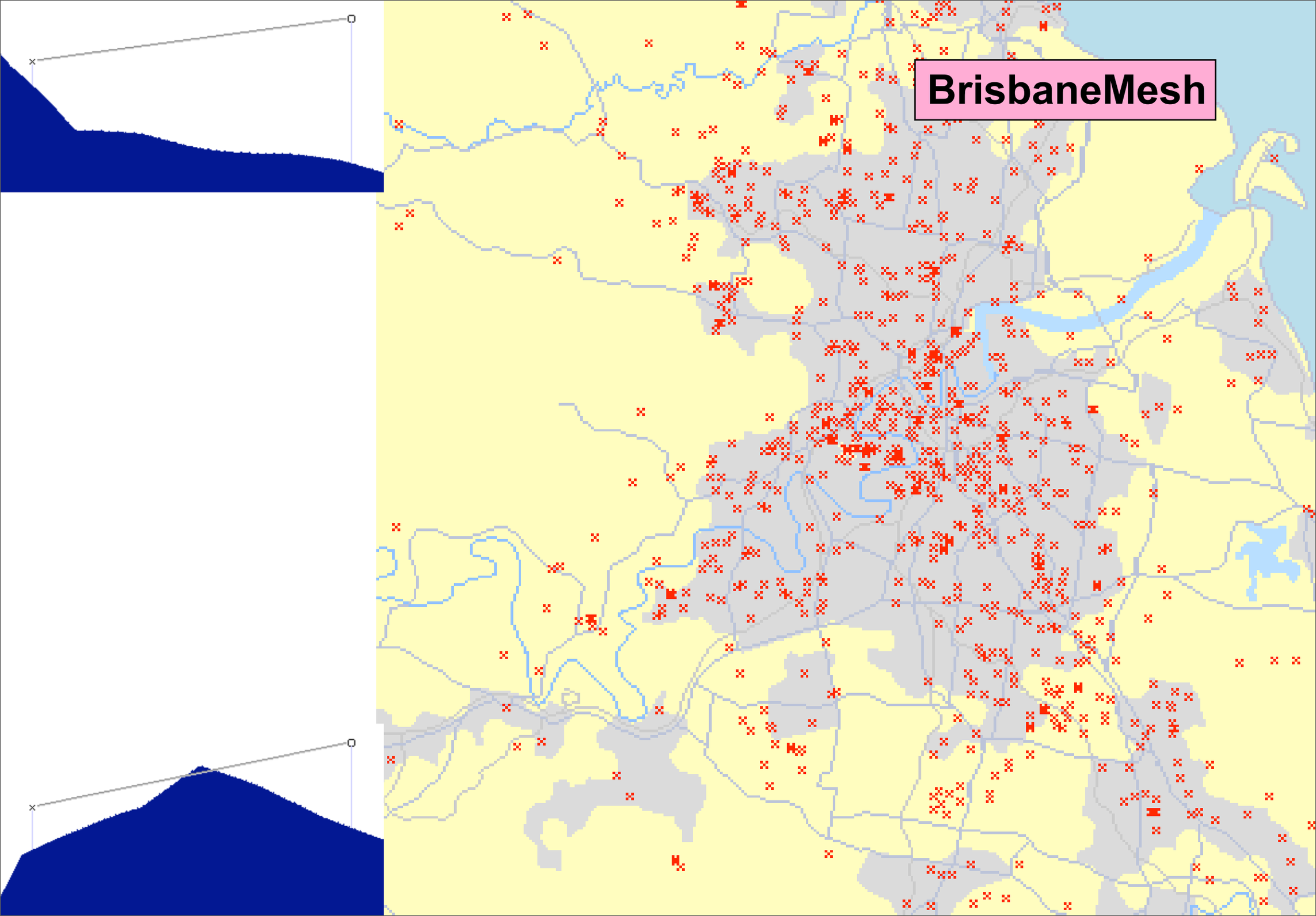
- Communication as supervised, regulated and deregulated, commercialized good
- Communication by us all and for us all

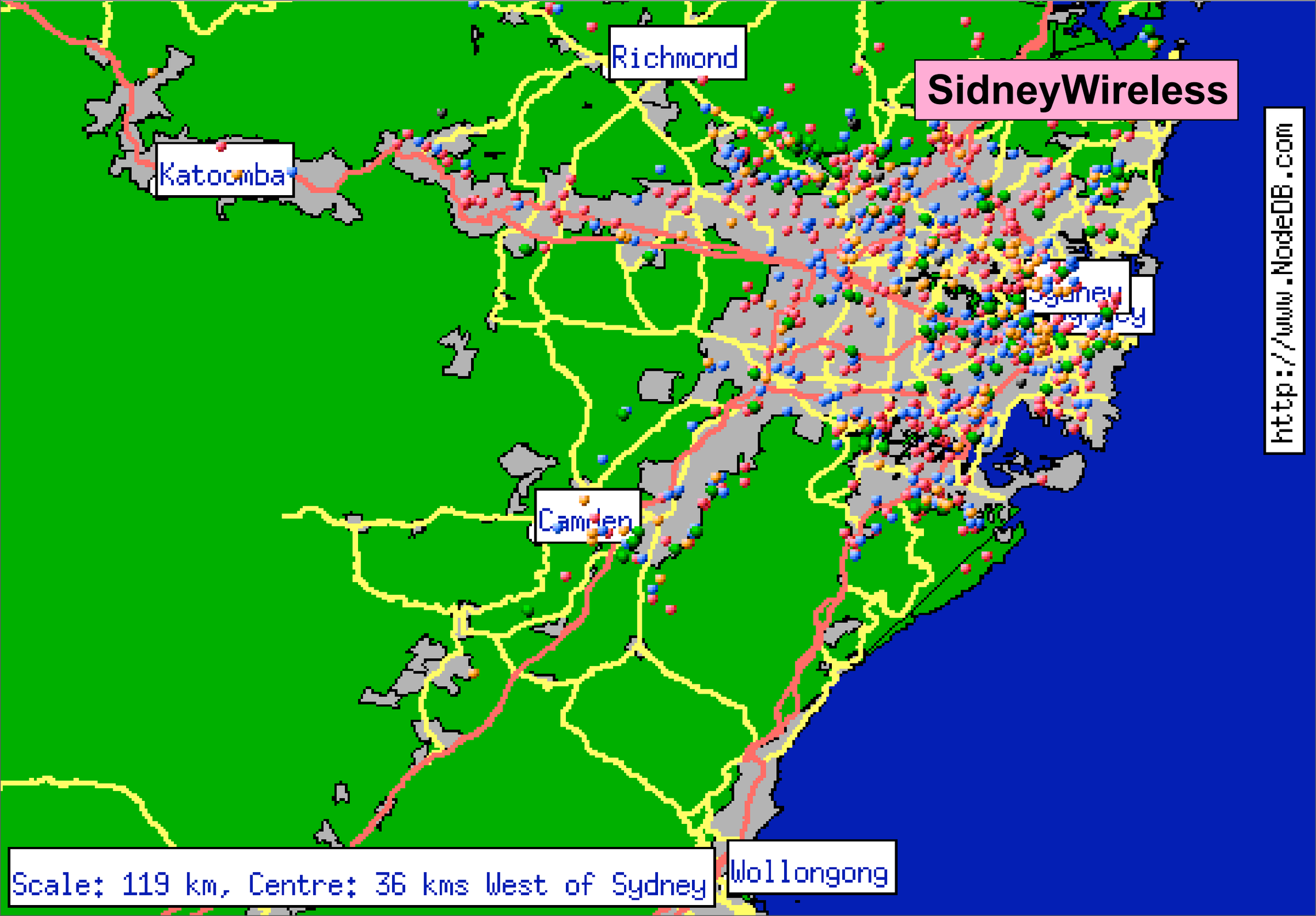
- Every bit pays (for the provider)
- Its out net, out infrastructure and our bits

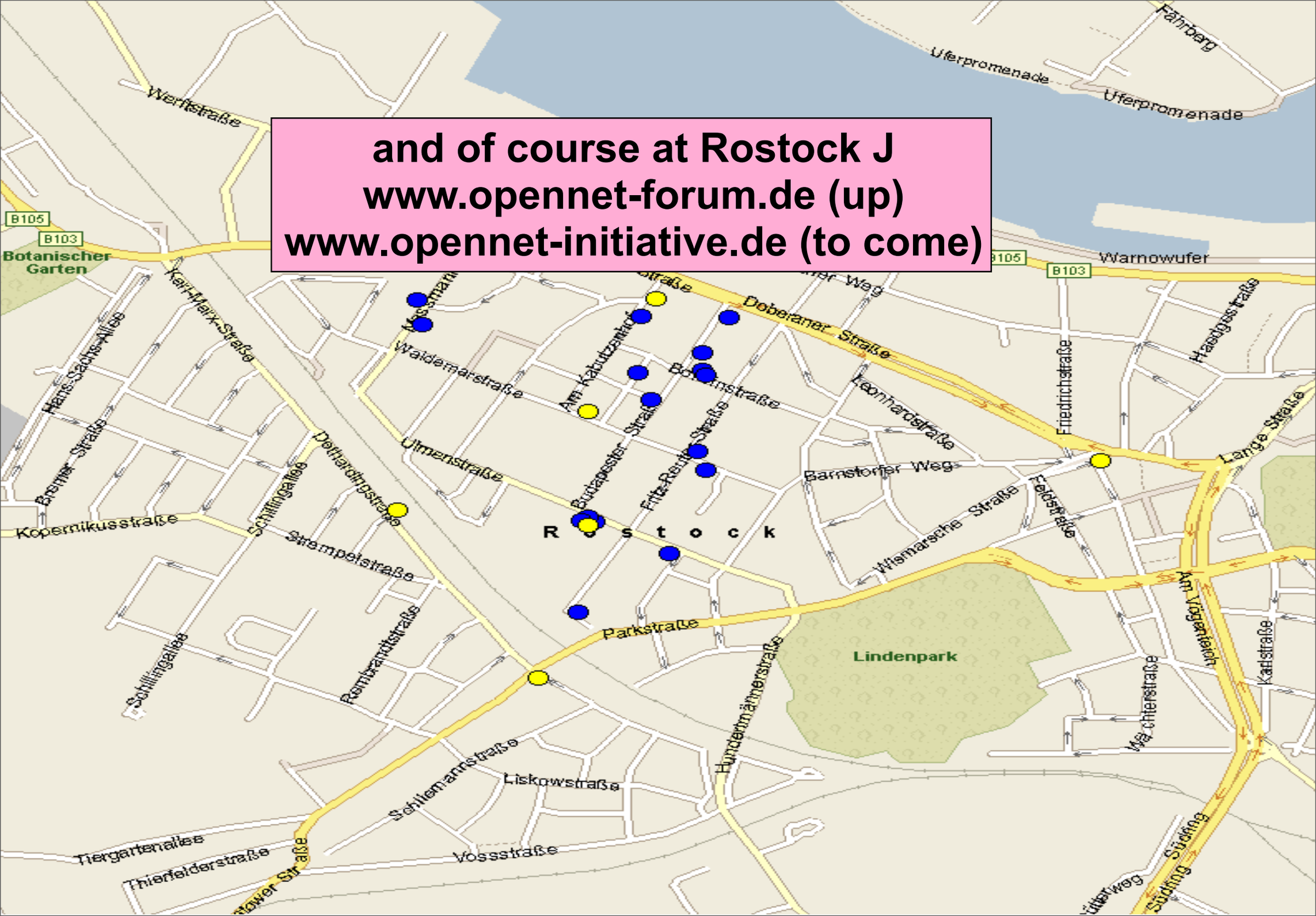

Djursland.net
Fase 1: Kørende
Fase 2: Sommer 2003
Fase 3: Sensommer 2003
Kæder


MIT Roofnet
Delivery Rates
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Last Updated: Thu Jun 17 17:15:34 EDT 2004


BerlinBackbone
yorken
sonne72
Wichert52
Lychener43
basque
FluxRadiator_db
chodo25_ma
SredZki40
Zion19
KuFa Moabit
In-Berlin
tuchol48
tacheles
bootlab
CCC
HdL
kma69_db
bbnet_db
Mattern3
databerlin_db
Tagen
kurtzz_db
suspiria
gabe1
nga81
berlinwireless
Mainzer24
ND
blackhole
RapunCell
rs10
c-base
Wede18
Box42
wue32
Libauer8
wue55
Holtei13
subnet
KargyBoy
leo34
Heine12
marla
Kohlfurter2
FalckenWeb_db
SoftHub_ma
s20f
Krül12
Bouche12
Beer8


BrisbaneMesh


SidneyWireless
Richmond
Katoomba
Camden
Wollongong
Scale: 119 km, Centre: 36 kms West of Sydney
http://www.NodeDB.com


and of course at Rostock J
www.opennet-forum.de (up)
www.opennet-initiative.de (to come)
Uferpromenade
Uferpromenade
Fährberg
Werftstraße
B105
B103
Botanischer Garten
Warnowufer
B105
B103
Doberaner Straße
Waldemarstraße
Am Kabutzenhof
Bussestraße
Leonhardstraße
Friedrichstraße
Hasdgestraße
Lange Straße
Barnstorfer Weg
Wismarsche Straße
Feldstraße
Ulmenstraße
Budapester Straße
Fritz-Reuter-Straße
Hans-Sachs-Allee
Karl-Marx-Straße
Bremer Straße
Kopernikusstraße
Schillingallee
Dethardingstraße
Strempelstraße
Rembrandtstraße
R o s t o c k
Parkstraße
Lindenpark
Hundermännerstraße
Am Vögenteich
Karlstraße
Wachtlerstraße
Schliemannstraße
Liskowstraße
Tiergartenallee
Thierfelderstraße
Vossstraße
Südring

Just a thought

Imagine WiMAX attached anonymous storage

For WLAN it‘s already there:

- Asus Spacelink 802.11g with 500 GB USB drive and anonymous ftp

Now add Freenet concepts encryption and anonymity

Question: How could one possibly & practically censor or „regulate“ this?

The big chance is Wimax

Yesterday: Cable

- Large investments
- Large distances
- Large data rates

Today: WLAN

- Low investments
- Medium distances
- Medium data rates

Tomorrow: WIMAX

- Low investments (hopefully: shared)
- Large distances
- Large data rates

But not at the same time L

100,-	Euro
200	Meter
2 - 54	Mbit / sec

100,-	Euro
50	Km
2 - 70	Mbit /

2004: First prototypes
2005: Chipset by Intel
2007: In every Laptop

What we can do (1)

Embrace technology

- **Understand** standard (complicated & solid 900+ pages)
- **Educate** ourselves
- Make experiences with **base stations** (not only with subscriber stations)
- Write **OO model** for API
- **Danger:** WiMAX stays closed & controlled know how (such as in GSM & UMTS)

Develop applications

- **Voice** over WiMAX
- **Games** over WiMAX (use broadcast features)
- **Community content** over WiMAX
- **Free, open, anonymous** layers for WiMAX
- **Must have many** open source – open content applications

What we can do (2)

Regulatory discussion

- **Must obtain** sufficient open spectrum for meshing and roaming
- **Must prevent** further regulation of applications
  eg: VoIP, key escrow, content censorship
- **Must deploy** anonymous & free content networks (Freenet, Eternity service, etc.)

TIME LINE

Opensource WiMAX

- **Experiment** with MAC and PHY APIs
- Write OO **model / simulator** for MAC and PHY API
- **Linux driver** for WiMAX adapters
- **Linux enhanced** WiMAX equipment (presently: FPGA & DSP, ASIC)
- **WiMAX enabled** Linux equipment

Just a thought

Imagine WiMAX attached anonymous storage

For WLAN it‘s already there:

- Asus Spacelink 802.11g with 500 GB USB drive and anonymous ftp

Now add Freenet concepts encryption and anonymity

Question: How could one possibly & practically censor or „regulate“ this?

Let us peek into the standard

PHY Layer

OFDM

- Which is a topic by itself

Dynamic Frequency Selection

- Chose a channel to combat interference
- In certain bands mandatory (military, radar)

Transmit Power Control

- Reduce EIRP so far as possible

Frequencies (1)

Table B.1—Frequency bands and channel allocation

Frequency bands (GHz) (licensed unless noted)		Allowed channel spacing	Reference
2.305–2.320 2.345–2.360		1 or 2 x (5 + 5 MHz) or 1 x5 MHz (Can be aggregated in any combinations) Interference Protection to DARS	USA CFR 47 part 27 (WCS) See FCC Docket IB95-91 for potential (increased) interference from DARS repeaters.
2.150–2.162 2.500–2.690		125 kHZ to (n x 6) MHz Single or multiple, contiguous or non-contiguous and combinations. Interference Protection to video and ITFS users	USA CFR 47 part 21.901 (MDS) USA CFR 47 part 74.902 (ITFS, MMDS)
2.150–2.160 2.500–2.596 2.686–2.688		1 MHz – (nx6) MHz (1 or 2-way) 25 kHz-(n x 25 kHz) "return" Contiguous channels preferred	Canada SRSP-302.5 (MCS) MDS service allocated to adjacent sub-bands (incl. separate "return" channels)
2.400–2.483.5 (license-exempt)		Frequency Hopping or Direct Sequence Spread Spectrum etc.	CEPT/ERC/REC 70-03 USA CFR 47 Part 15, subpart E [B19]
3.400–4.990	3.410–4.200	1.75–30 MHz paired with 1.75 MHz to 30 MHz Symmetric only. (50 MHz or 100 MHz separation)	Rec. ITU-R F.1488 Annex II ETSI EN 301 021[B18], CEPT/ERC Rec. 14-03 E, CEPT/ERC Rec. 12-08 E
	3.400–3.700	n x 25 MHz (single or paired) (50 MHz or 100 MHz separation if paired)	Rec. ITU-R F.1488 Annex I CITEL PCC.III/REC.47 (XII-99) Canada SRSP-303.4 (BWA)
	3.650–3.700	Rulemaking in progress	USA FCC Docket WT00-32
	4.940–4.990	Rulemaking in progress	USA FCC Dockets WT00-32 and ET-98-237

Not so easy
- **even if restricted to the US view**
- **and restricted to 2 – 11 GHz**

Frequency bands (GHz) (licensed unless noted)		Allowed channel spacing	Reference
5.150–5.850 (license-exempt)	5.150–5.350	n x 20 MHz (HIPERLAN) Restricted to Indoor Use	CEPT/ERC/REC 70-03
	5.470–5.725	n x 20 MHz (HIPERLAN)	
	5.250–5.350	100 MHz Max. Restricted to Indoor Use	USA CFR 47 Part 15, subpart E [B19] USA CFR 47 Part 15, subpart C [B19]
	5.250–5.350	100 MHz Max	
	5.725 –5.850	125 MHz Max	
10.000–10.680		3.5 to 28 MHz paired with 3.5 to 28 MHz. Symmetric only 350 MHz separation	CEPT/ERC/REC. 12-05 ETSI EN 301 021 [B18]

Frequencies (2)

Licensed 2.5 GHz

- Already allocated in US, Mexico, Brazil, Asia
- Ongoing efforts in other countries

License exempt 5 GHz

- License free in the US
- Ongoing efforts for opening this in other countries

Licensed 3.5 GHz

- Licensed in more than 100 countries
- Generally requires license

Others to be harmonized soon

Still an open question

Frequencies (3)

Just what is a license?

Austria: Auctioned License

- 17 Frequency allocations (3.5 Ghz band)
- Held by 4 companies
- Auctioning yields total amount of 464.000 Euros

Germany: Licensing Light

- No auctioning (too expensive)
- No formalized process (too inflexible)
- In case of frequency conflict: Look for local, pragmatic solution

Modulation Schemes Used

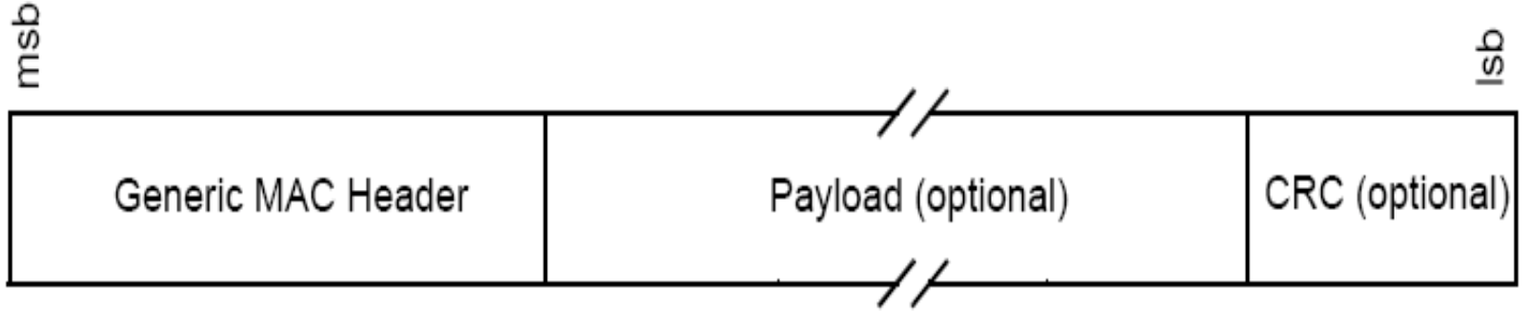
	802.16	802.16a	802.16e
Modulation	QPSK 16 QAM 64 QAM	OFDM 256 QPSK 16 QAM 64 QAM	QPSK 16 QAM 64 QAM
Bit Rate	32 – 134 Mbps at 28 MHz Channelization	< 75 Mbps at 20 Mhz Channelization	< 15 Mbps at 5 MHz Channelization
Channel Bandwidths	20, 25 and 28 MHz	Selectable 1.25 to 20 MHz	20, 25 and 28 MHz

Downlink Frames

Downlink Frame consists of

1. A **preamble** for synchronization
2. A **downlink map** telling the subscriber which part of the payload is intended for it
3. An **uplink map** telling the subscriber when it may access the air
4. A **payload**

MAC Layer



Generic MAC Header

Payload

Optional CRC (32 bit CCITT standard)

Payload can contain

- **Additional headers (depends on type field in Generic MAC Header)**
- **MAC management messages**
- **User Data**

MAC Layer
Generic Mac Header

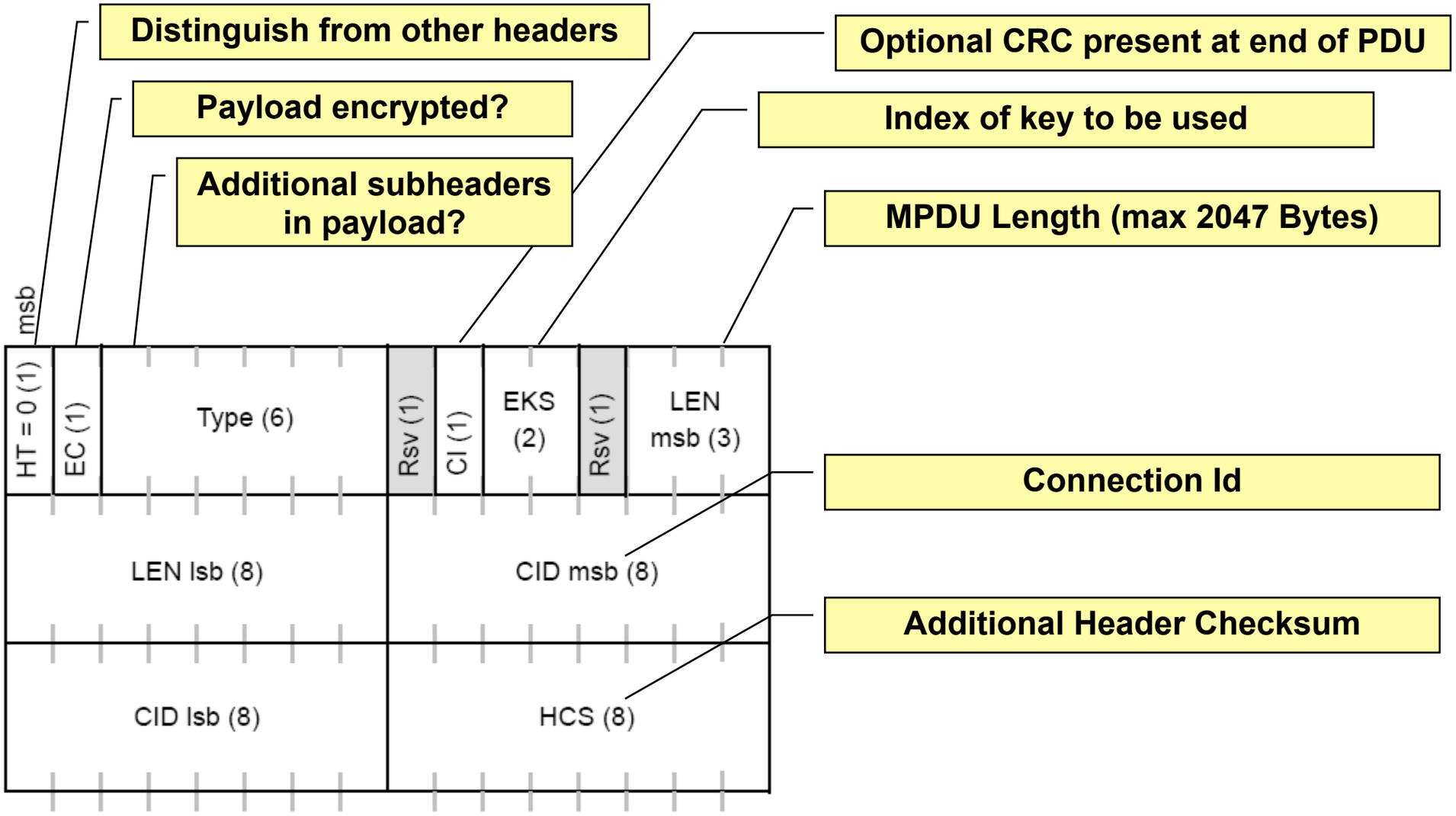


Figure 22—Generic MAC header format

MAC Layer
Oberservations based on Generic Header

MAC PDU length less than 2k Bytes

- But fragmentation and packing options are available

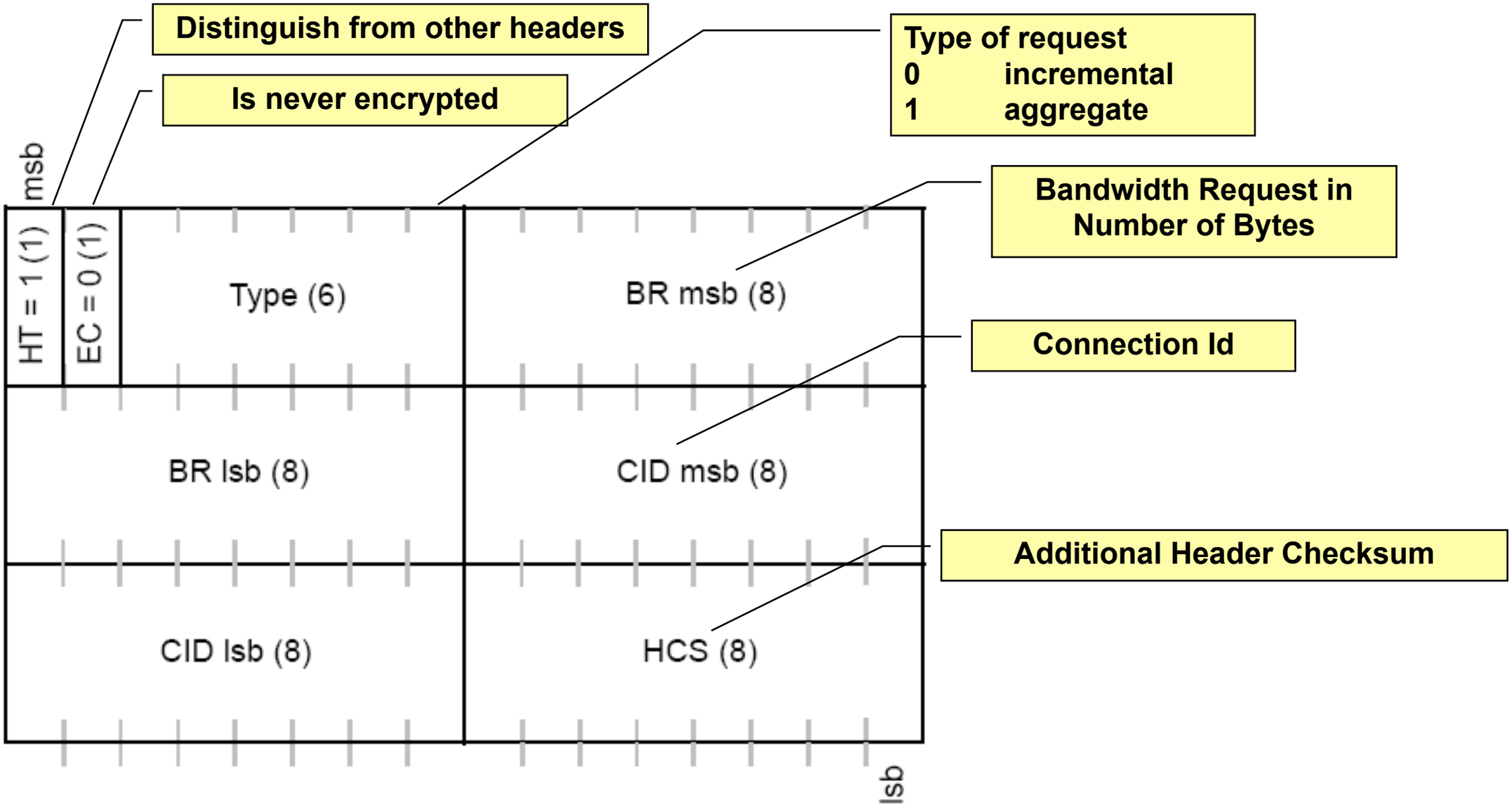
More than one encryption key can be active

- We have to say which one we want to use
- We must change keys from time to time
- But during the change of one key we always have another valid key
- So we do not spend (much) time on rekeying overhead

Basic item of management is the connection

- Compare TCP: Connection ID is 4-tuple of (IP1, Port1, IP2, Port2)

MAC Layer
Bandwidth Request Header



MAC Layer
Observations based on Bandwidth Request

Bandwidth requests come as a header

- As part of an empty payload
- Piggyback as part of a payload (even of a different connection id to the same subscriber)

Bandwidth requests are never encrypted

- Which is not a safe idea (and they are not authenticated either !)
- Which is more convenient since everyone sees the bandwidth requests

Note: A bandwidth request is given in bytes not in bytes per time unit

- Which is an abuse of language, but otherwise fine

Request type can be incremental or aggregate

- incremental (what subscriber needs in addition)
- or aggregate (what subscriber needs in total)
- Choice makes life easier for the streaming people

MAC Layer
Packing and Fragmentation

Fragmentation (Splitting MAC level packets)

- A MAC SDU can be broken into individual parts
- The parts are transmitted independently
- Indication is done by a special subheader

Packing (Aggregating MAC level packets)

- Multiple MAC SDUs or even fragments can be packed into one SDU
- Indication is done by a special subheader

Advantages

- More efficient use of available slots
- Bandwidth requests can be issued earlier

Network Entry

Getting access to the network

- Subscriber scans for downlink from Base and synchronizes PHY
- Subscriber identifies free uplink slot
- Subscriber informs Base of its capabilities and presence
- Primary management connections are established
- Subscriber provides proof of authorization
- Key exchange protocols establish valid keys
- Secondary management connections are established
- Adaption layers are configured (eg: IP)

Keeping access to the network

- Periodic exchange of management messages
- Check channel condition
- If necessary, switch PHY or start handoff (for mobile users)

Security Sublayer

Identification of the Subscriber

- Asymmetric keys with PKI and certificate structure

Authentication Key AK

- Symmetric key for distributing and deriving further keys

Key Distribution Key KEK

- Derived from Authentication Key
- Used to distribute Traffic Encoding Key

Traffic Encryption Key

- Used to encrypt traffic

Double Layer Hybrid Approach

Problem 1: **Asymmetric encryption takes too much CPU power**

Solution 1: **Encrypt symmetric key with asymmetric method**
Symmetric methods are faster
Occasionally provide a new symmetric key

Problem 2: **Providing a new symmetric takes too much CPU power**

Solution 2: **Introduce another layer of indirection**
Key redistribution is faster
Occasionally provide a new key at both levels

Result

- Need a two layered key-distribution / re-keying approach
- That is esenntially the contents of the Privacy sublayer

Problems left

Base not authenticated, allows man-in-the-middle

MAC header not encrypted, allows attacks & fakes on MAC headers

MAC Management Messages not encrypted, allows attacks & fakes on Messages

Main (or only?) focus is protection against theft of service

Permissions bound to MAC address of subscriber instead of to user

Subscriber based production of certificates not described, allows attacks on randomization scheme and key generator

Subscriber may have factory installed keys (which might be escrowed)

Security generally is handled by the operator and by the base station thus scheme requires trusting the operator and the base station

Standard is not fully clear and not sufficiently formally defined

There are not yet fully compliant and certified products

... but there are already papers describing the weaknesses of the security

Angry remark concerning security

IEEE did not get WEP security right

IEEE did not get Wimax security right

NSA must love the security guys from IEEE,

since they make their work much easier

The newest standard documents in PDF format are sold for $$$

and are protected by a node locked digital rights management

- **The department bought one for my computer at work**
- **The department bought a second one after my motherboard went dead**
- **I bought a third for my first computer at home**
- **I would need a fourth one to take along with my laptop**
- **And after a minor reconfiguration of my two PCs at home I spent 2 hours undoing the relevant changes to be able to read my third copy again**

Why?

Why does a professional institution

living from the dues of their members

seem to

always

get the wrong things right

and the right things wrong

when it comes to security

For the marketing people

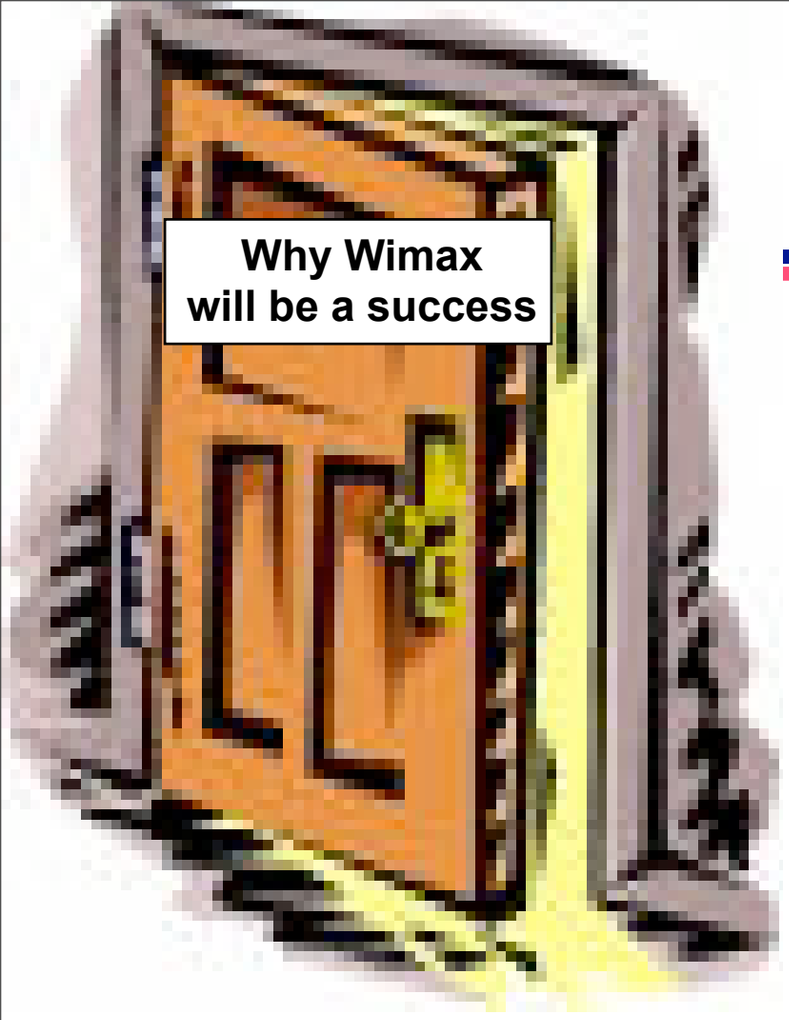
Tons and tons of marketing studies

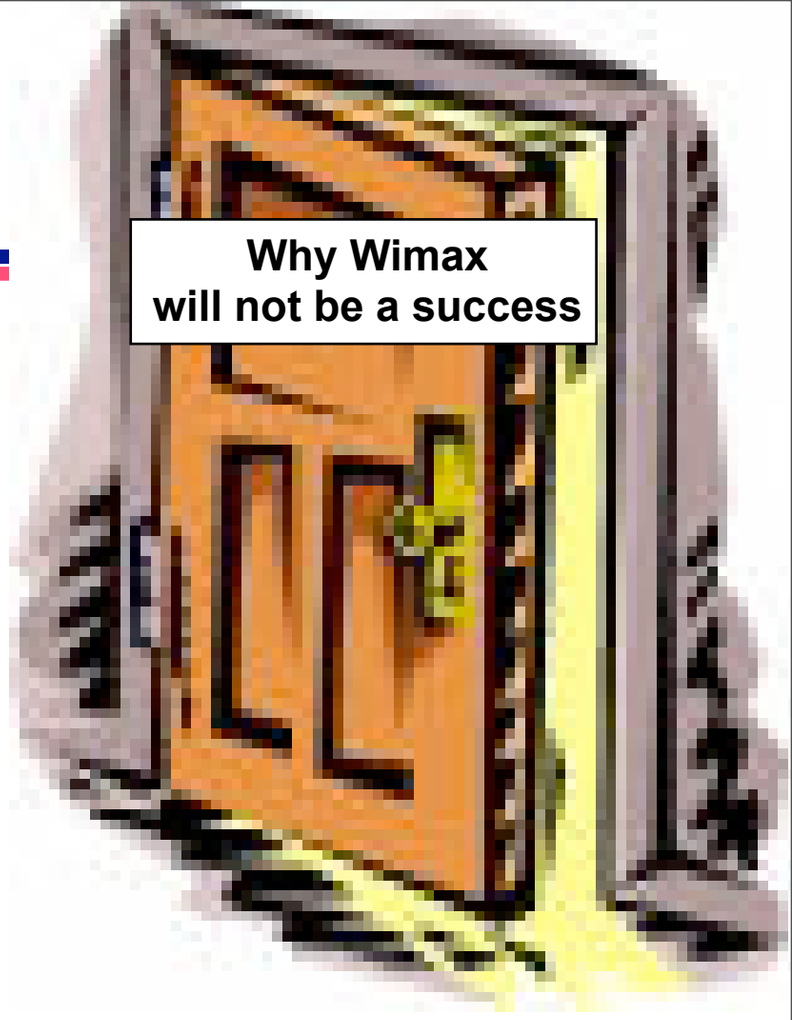
Found on the web:

„Wimax presently is discussed in terms of dollars and market opportunities, not in terms of equipment or solutions“

Presently the best way to make money on Wimax is to publish a study on how to make money on Wimax

Clemens H. Cap
http://wwwiuk.informatik.uni-rostock.de
http://www.internet-prof.de


Why Wimax
will be a success


Why Wimax
will not be a success

Why Wimax will be a success

Good Standard: IEEE Standard and Wimax interoperablility Certification

Well regulated: Development accompanied by evolution of frequency regulation

Technics:

- Broadband speed for NLOS
- High number of simultaneous sessions
- Support for mobility, roaming and meshing
- High spectral efficiency
- Good quality of service

Demand

- Demanded by carriers
- Solves last mile problem
- New deployment models

Why Wimax will not be a success

No products: The products are coming too late

No proof of product yet

Regulation: Is going on but no clear cut and reliable results yet

Counter demand:

- The UMTS guys and the license / auction fees they had to pay

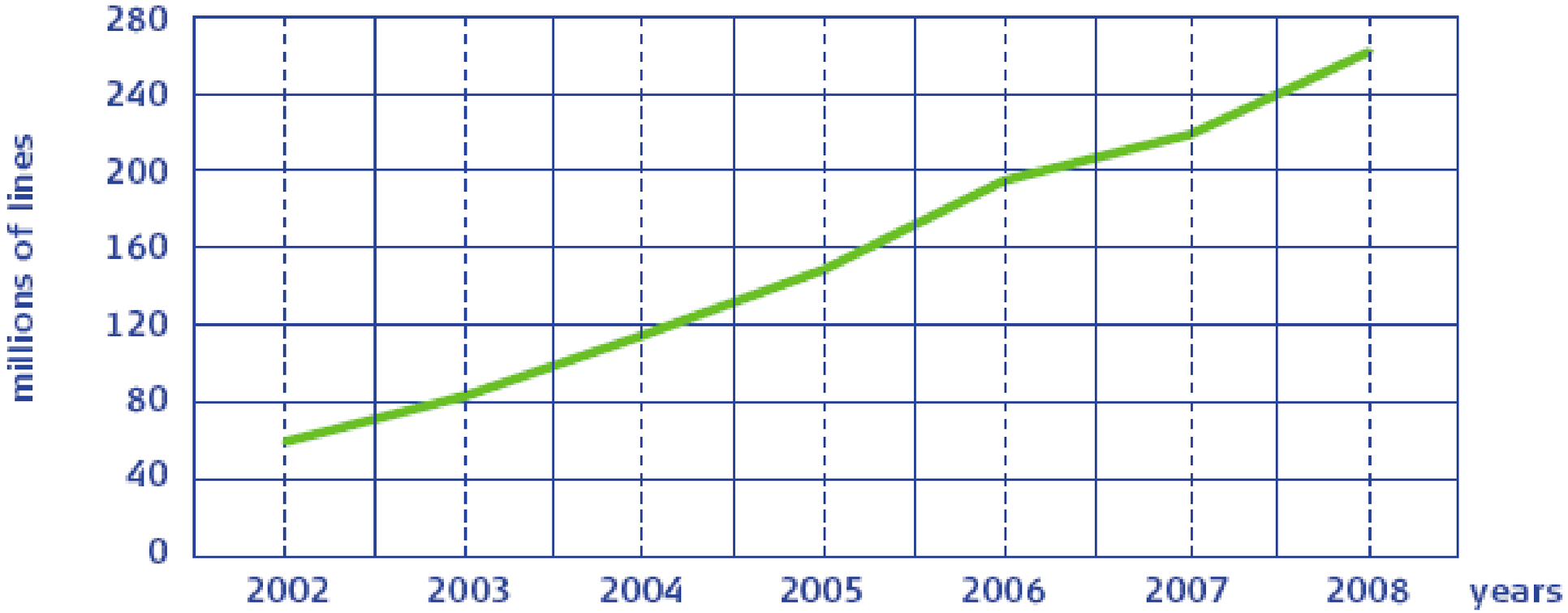
Development: Yet another hype to break down early enough to ruin many?

Expectations already risen too high? (NLOS to 70 km at 100 Mbits for 1$)

Unresolved issues:

- Free spectrum applications?
- High frequency devices (66 GHz)?
- Handoff into WLAN, UMTS, GSM

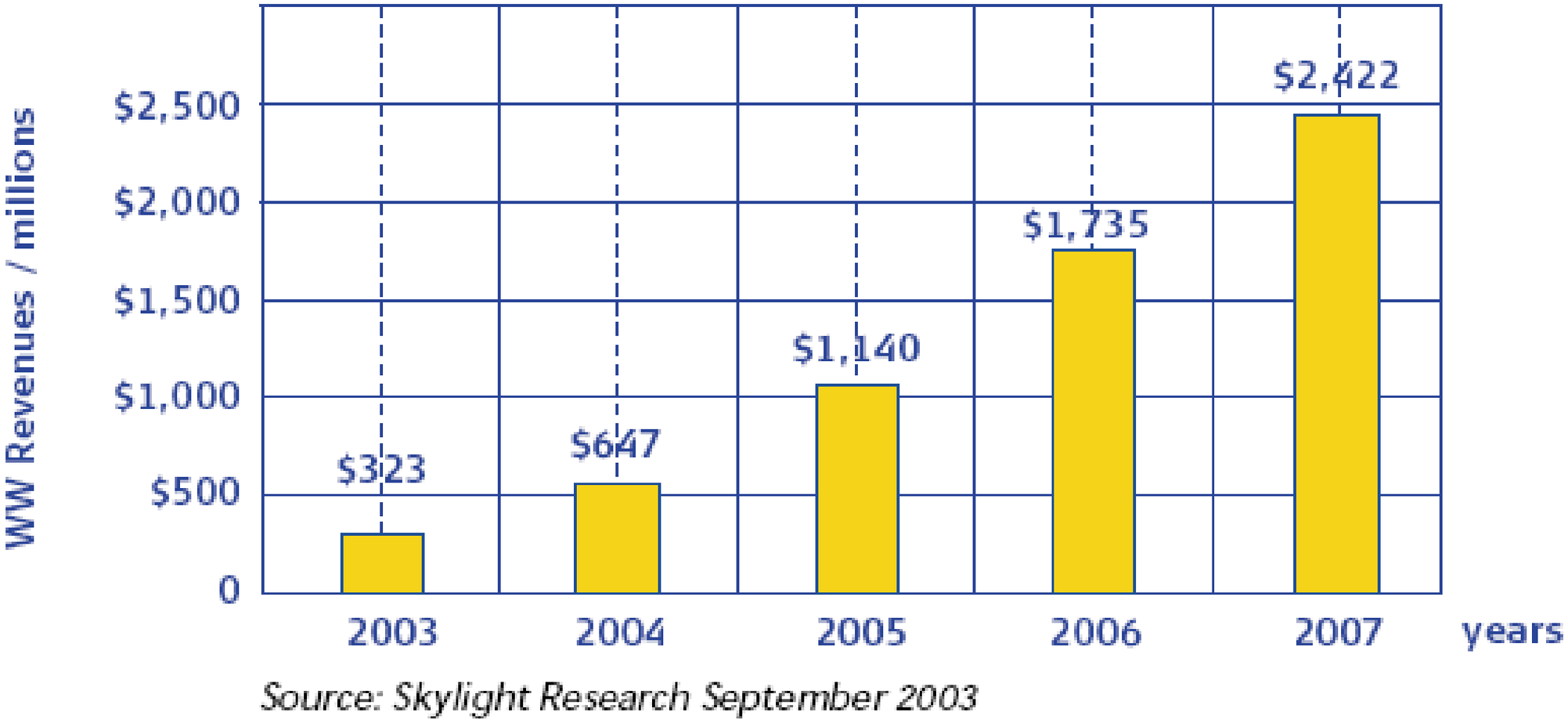
Market Expectations for wired broadband



Source: Allied Business Intelligence Inc 2003

World Wide Number of Broadband Wires

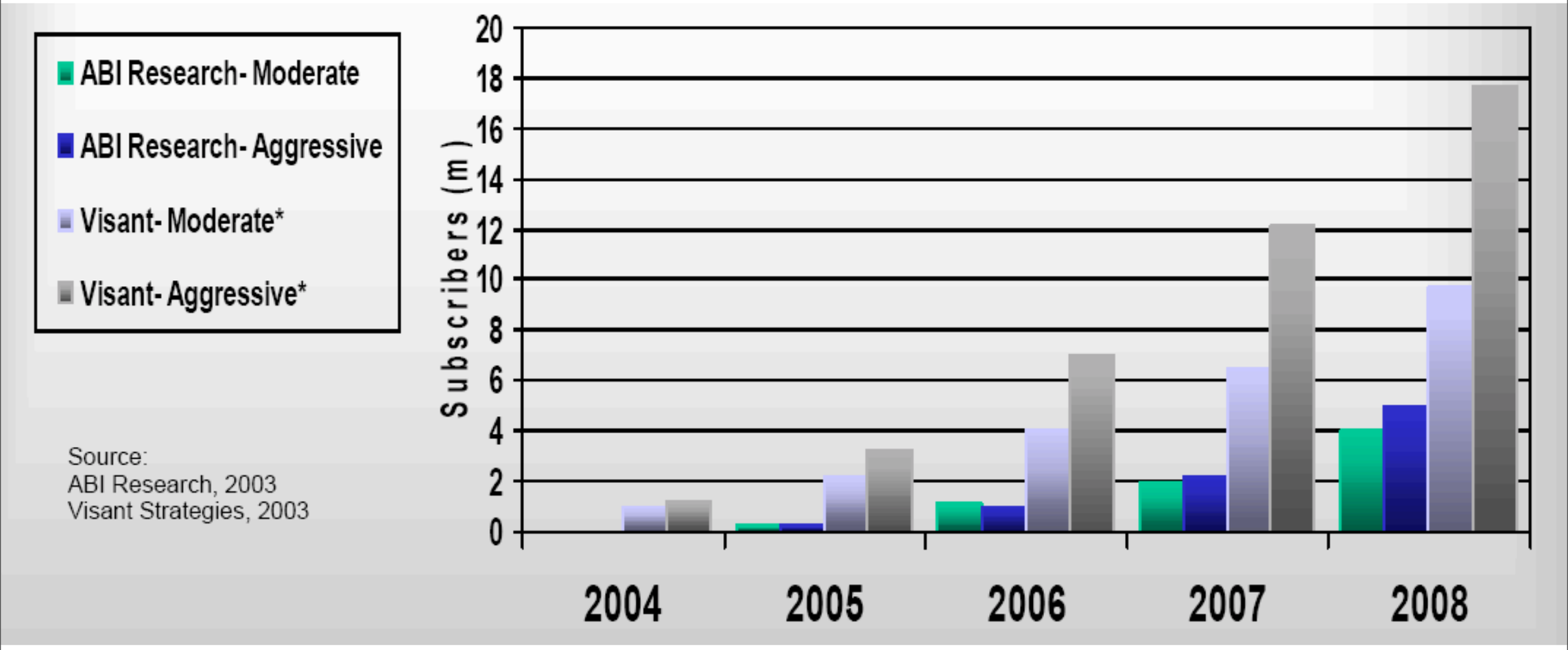
Market Expectations for wireless broadband



Source: Skylight Research September 2003

World Wide Revenues from Point to Multipoint Broadband Wireless Access

Market Expectations for number of subscribers



Source:
ABI Research, 2003
Visant Strategies, 2003

Equipment

Basestations and Subscriber Stations

- Redline Communications — First Base Station
- Alvarion BreezeMAX — ETSI HiperMAN compliant

Road Map

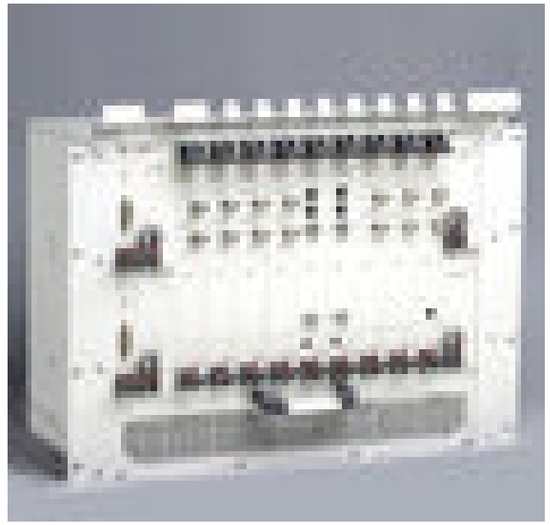
- Chipset (Intel Rosedale / Centrino 2; Wavesat)
- Adapters
- Motherboard Modules
- Mobile phones, laptops, PDAs

Alvarion

Product Line BreezeMAX

Base Station Equipment

- **Modular concept: Several components for a 19“ rack**
- **One component for every sector served**
- **Separation indoor access unit and outdoor amplifier unit**
- **Micro base station available for rural areas**



Customer Premises Equipment (CPE)

- **Broadband Data CPE**
- **Broadband Voice CPE**

Redline Communications

30 series

50 series

- Pre 802.16 systen

100 series

- Claims to be first fully 802.16 compatible system
- Presently only basestation