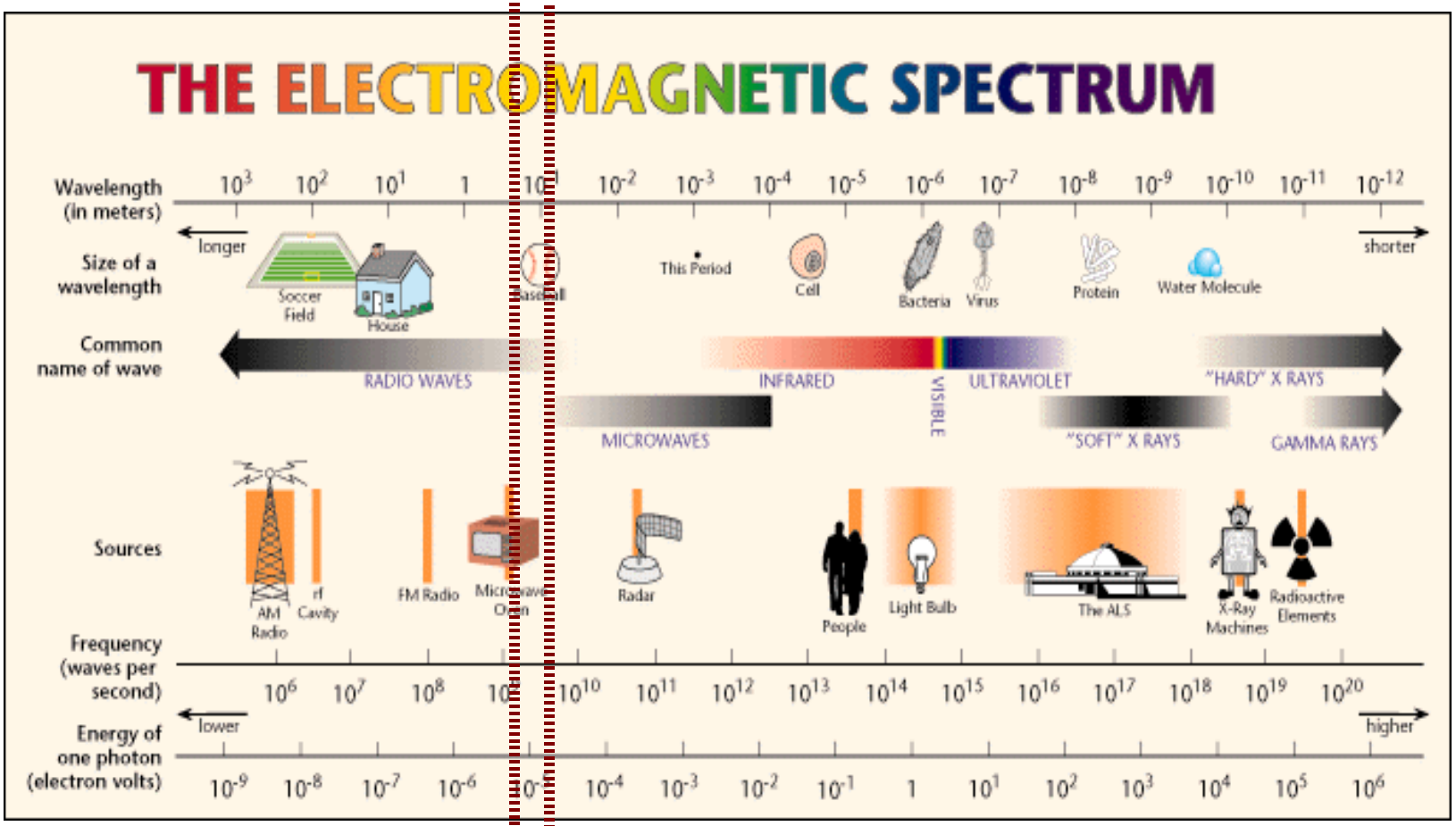
802.11 Technical Introduction

Tomas Krag
t@wire.less.dk

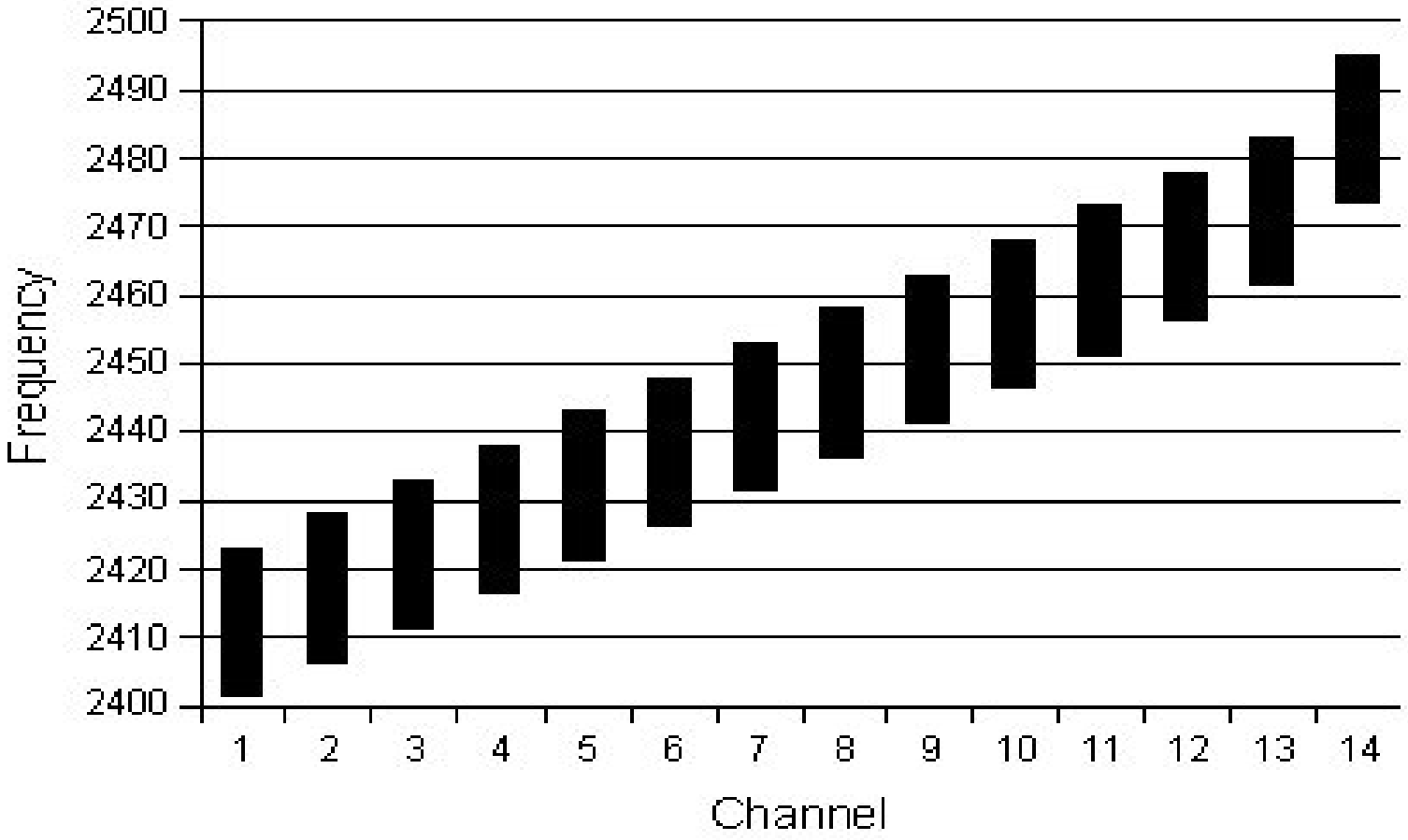
Unlicensed Spectrum

- There was a need for spectrum with fewer regulations
- The ISM band at 2.4 Ghz & 5.2 GHz
- The UNII band at 5.8 GHz
- No need for a per radio license
- Rules define what is legal in these bands

Electromagnetic Spectrum



802.11 in 2.4 GHz



The Standards Organisations

- FCC
  - Federal Communications Commission
- IEEE
  - Institute of Electrical and Electronics Engineers
- ITU-T
  - International Telecommunications Union
- ETSI, IETF, ISO etc.

802.11 Alphabet soup

- The main communications standards
  - 802.11
  - 802.11b
  - 802.11g
  - 802.11a
  - *802.11n*
- The alphabet soup
  - 802.11 d, e, f, g, h, **i**, j, p, r, s, t, u, v, w

The IEEE 802.11 Reality

Standard	*Freq*	*"speed"*	*status*	*modulation*	*comments*
	2.4GHz	2 Mbps	rel mid-90's	FHSS, DSSS	Defined for microwave and Infrared
a	5 Ghz	54 Mbps	rel 1999, market 2002	OFDM	(Orthogonal Frequency Division Multiplexing)
b	2.4 Ghz	11 Mbps	rel 1999, market 2001	DSSS	High Rate DSSS in the 2.4GHz band
g	2.4 Ghz	54 Mbps	rel 2002, market 2003	OFDM, PBCC	Higher Rate Extensions in the 2.4GHz Band
n		up to 600 Mbps	draft ratified january 2006	OFDM	MIMO (Multiple-in, Multiple Out) extensions to existing standards

802.11 in the network stack

Layer	ISO	802.11
7	Application	
6	Presentation	
5	Session	
4	Transport	
3	Network	
2	Data link	802.11 MAC
1	Physical	802.11 PHY

The 802.11 Protocol Stack

<table>
<tr><td rowspan="5">802.1
Management</td><td colspan="7">802.2 Logical Link Control</td><td>Data Link Layer</td></tr>
<tr><td colspan="7"></td><td>LLC Sublayer</td></tr>
<tr><td>802.3</td><td>802.5</td><td colspan="5">802.11</td><td></td></tr>
<tr><td rowspan="2">802.3
MAC</td><td rowspan="2">802.5
MAC</td><td colspan="5">802.11 MAC</td><td>MAC sublayer</td></tr>
<tr><td>802.11
FHSS
PHY</td><td>802.11
DSSS
PHY</td><td>802.11a
OFDM
PHY</td><td>802.11b
DSSS
PHY</td><td>802.11g
OFDM
PHY</td><td>Physical Layer</td></tr>
</table>

802.11 Terms

- Ad-hoc mode vs. Infrastructure mode
- Access Point (AP) vs. Station (STA)
- Service Set Identifier (SSID)
  - BSS, ESS, IBSS

AP: Access Point

Device that contains IEEE 802.11 conformant MAC and PHY interface to the wireless medium, and provides access to the distribution system for associated stations.

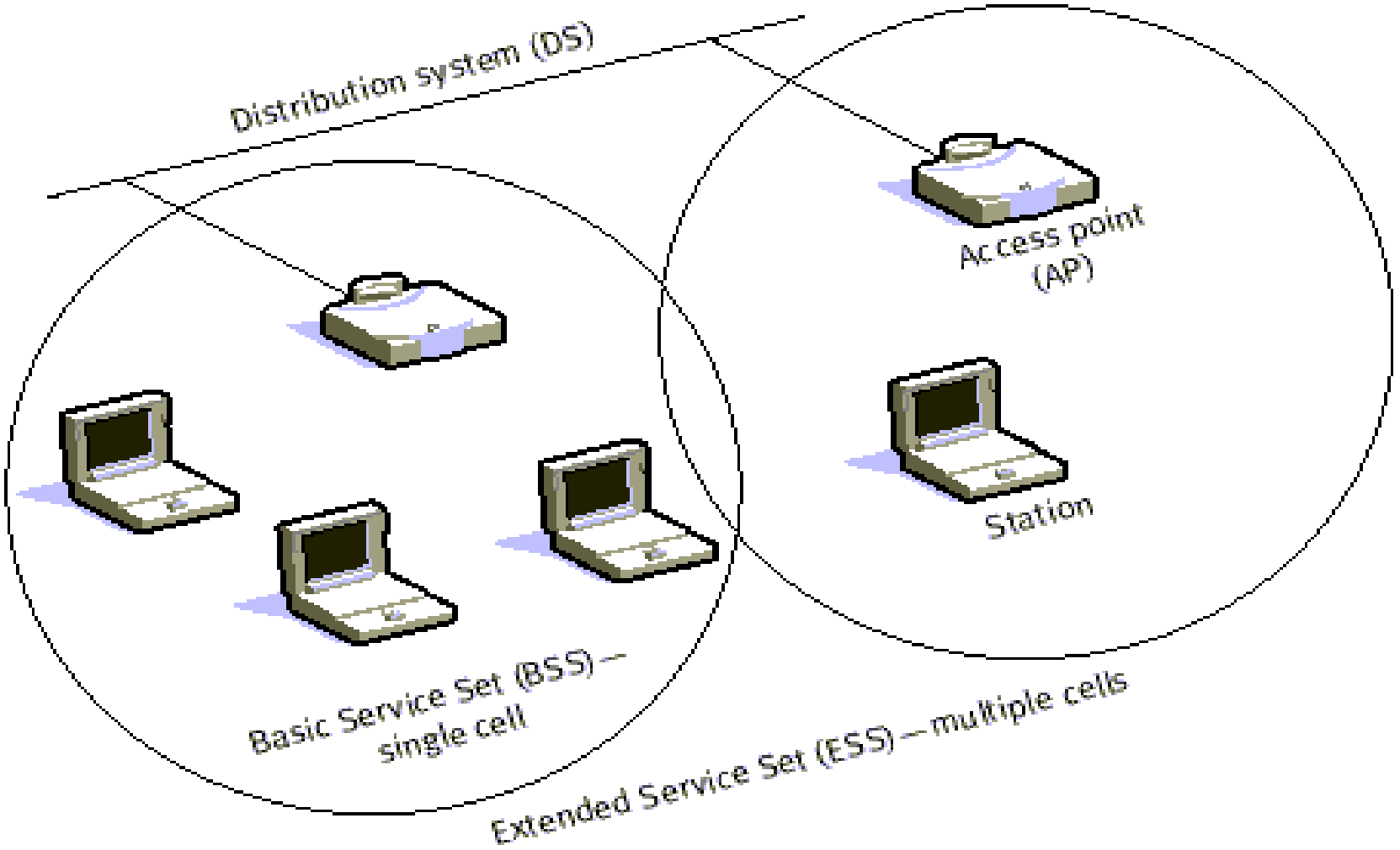
- Infrastructure Mode
- Linux: Master Mode

STA: Station

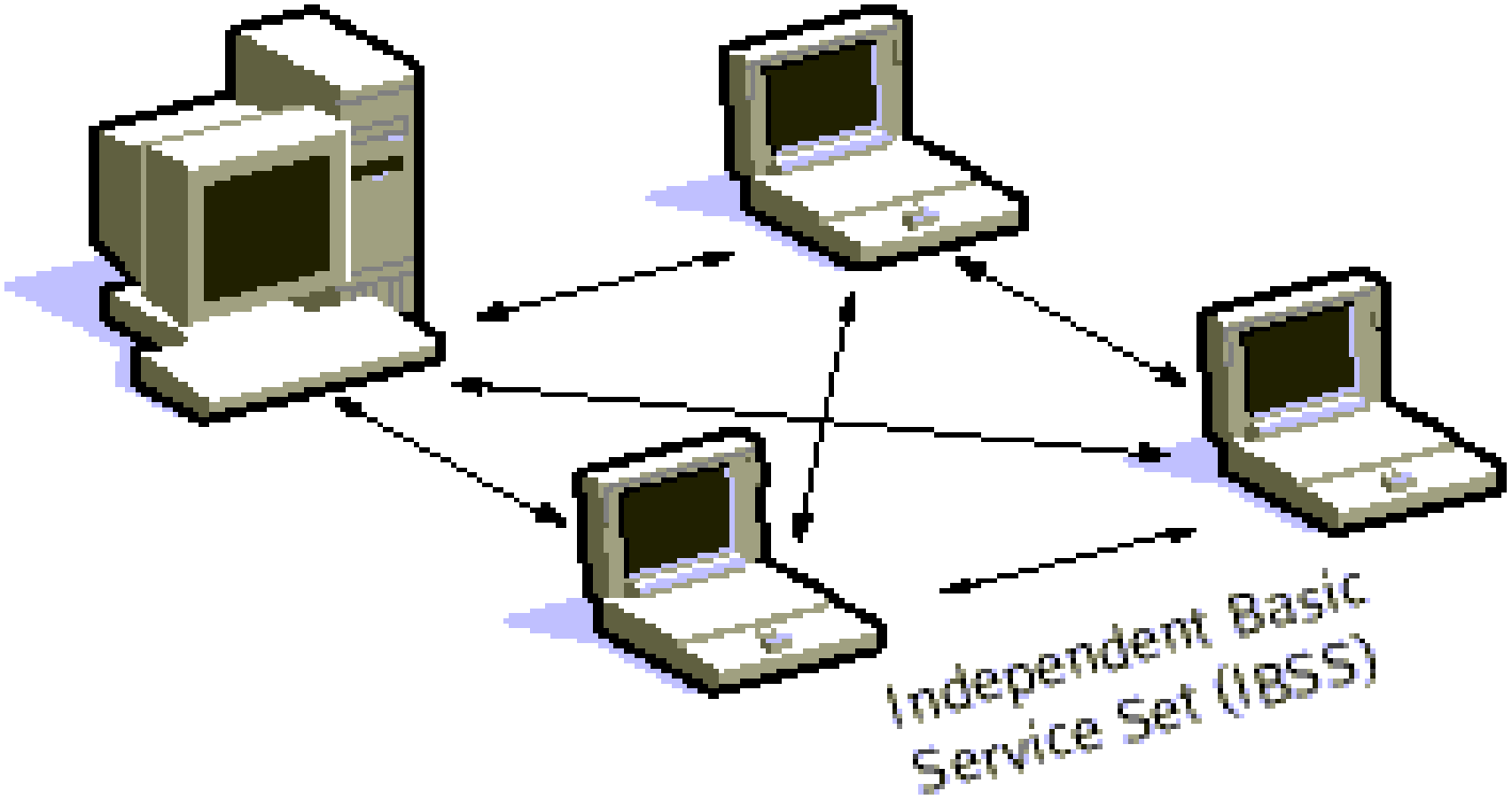
Device that contains IEEE 802.11 conformant MAC and PHY interface to the wireless medium, butdoes not provide access to a distribution system.

- Client
- Linux: Managed Mode

Infrastructure Mode



Ad-hoc Mode



BSS, IBSS and ESS

- BSS – (Basic Service Set)
  - A set of stations controlled by a single "Coordination Function" (the logical function that determines when a station can transmit or receive.
  - Similar to a cell in GSM network
  - Can be with or without an access point

BSS, *IBSS* and ESS

- IBSS - (Independent Basic Service Set)
  - A BSS which forms a self-contained network in which no Distribution System is available
  - A BSS with no access point
  - (Ad-hoc Mode)

BSS, IBSS and *ESS*

- ESS - (Extended Service Set)
  - A set of one or more BSS interconnected through a Distribution System.
  - There must be an Access Point that connects to the Distribution System

SSID and BSSID

- SSID - (Service Set Identifier)
  - Network Identifier
  - 32 octets
  - Each network (ESS or IBSS) has one SSID
- BSSID
  - cell identifier
  - 6 octets (looks like a MAC address)
  - Equivalent to mac-address of Access Point)

Questions?