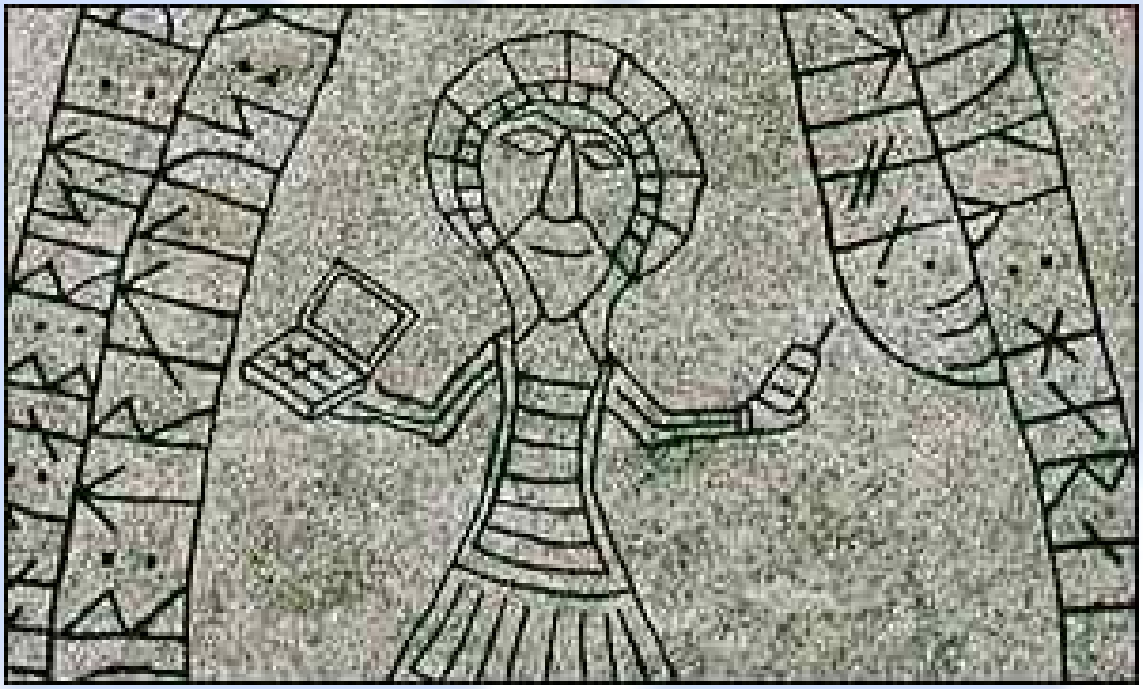
Blåtann / 802.15 (WPAN)

Lars Strand (lars at unik.no)
Andreas Tønnesen (andreto at unik.no)



Umiddelbare spørsmål:

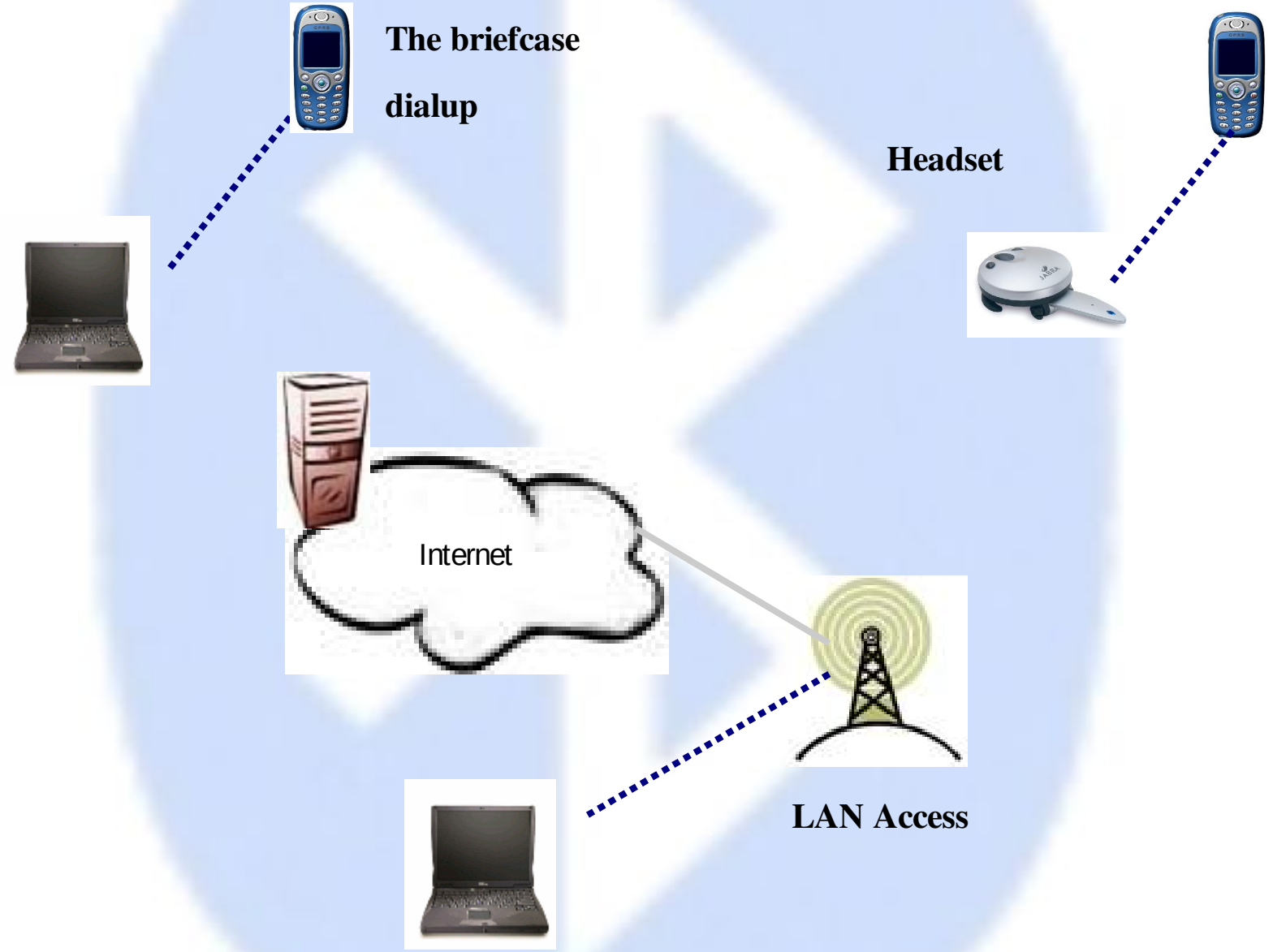
* Hvorfor blåtann fremfor wlan?
* Hvorfor blåtann fremfor vanlig kabling?
* Hvordan snakker enhetene sammen?
* Hvordan fungerer blåtann sammen med IP?
* Kan vi koble flere blåtann-nett sammen?
* Multihopp?
* Hva med sikkerhet?
* WPAN fremfor WLAN?

Hva? / Hvem?

* ment å lette bruk av enheter som krever tilkobling
  - fjernkontroll til TV/garasjeport/stereo
  - sync av PDA'er
  - trådløs telefon
  - stereoanlegg snaker med andre enheter (TV, video)
  - telefon til headset

* Bluetooth special intrest group (B-SIG)
  - grunnlagt av Ericsson, IBM, Nokia, Intel og Toshiba i 1998
  - i dag: over 2000 aktører med alle de store telekom. Aktørene, bla. 3Com, MS, Motorola ++

Scenarioer



THALES

The group shot above includes (clockwise starting from the top left):

3COM USB adapter; AnyCom Bluetooth CompactFlash Card, with PC Card adapter

on the right; BlueGear USB Bluetooth adapter; TDK USB Bluetooth adapter; TDK Blue5 Bluetooth adapter (for Palm V series PDAs); 3COM Bluetooth Wireless PC Card; and (in the middle) a Palm SD I/O Bluetooth adapter.

THALES

Spec:

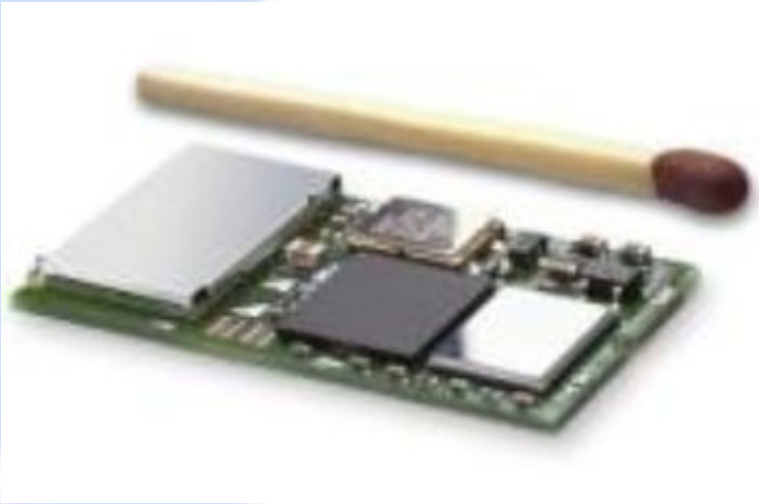
* spredt spektrum frekvenshopping
  - 79 frekvenser 1600 ganger i sek.
  - 3200 ganger i sek. ved søking etter andre enheter
  - 2.45GHz

* tre klasser/versjoner etter hvor mye strømforbruk:
  - class 3: 1mW, rekkevidde 0.1 - 10m
  - class 2: 1-2.5mW, rekkevidde ~10m
  - class 1: >100mW, rekkevidde ~100m

* handshake + header tar ~20% overhead(!)

Spec (2):

* 2000:
  - krets prototype på 0.9cm2
  - pris ~200kr
  - mindre krets under utvikling

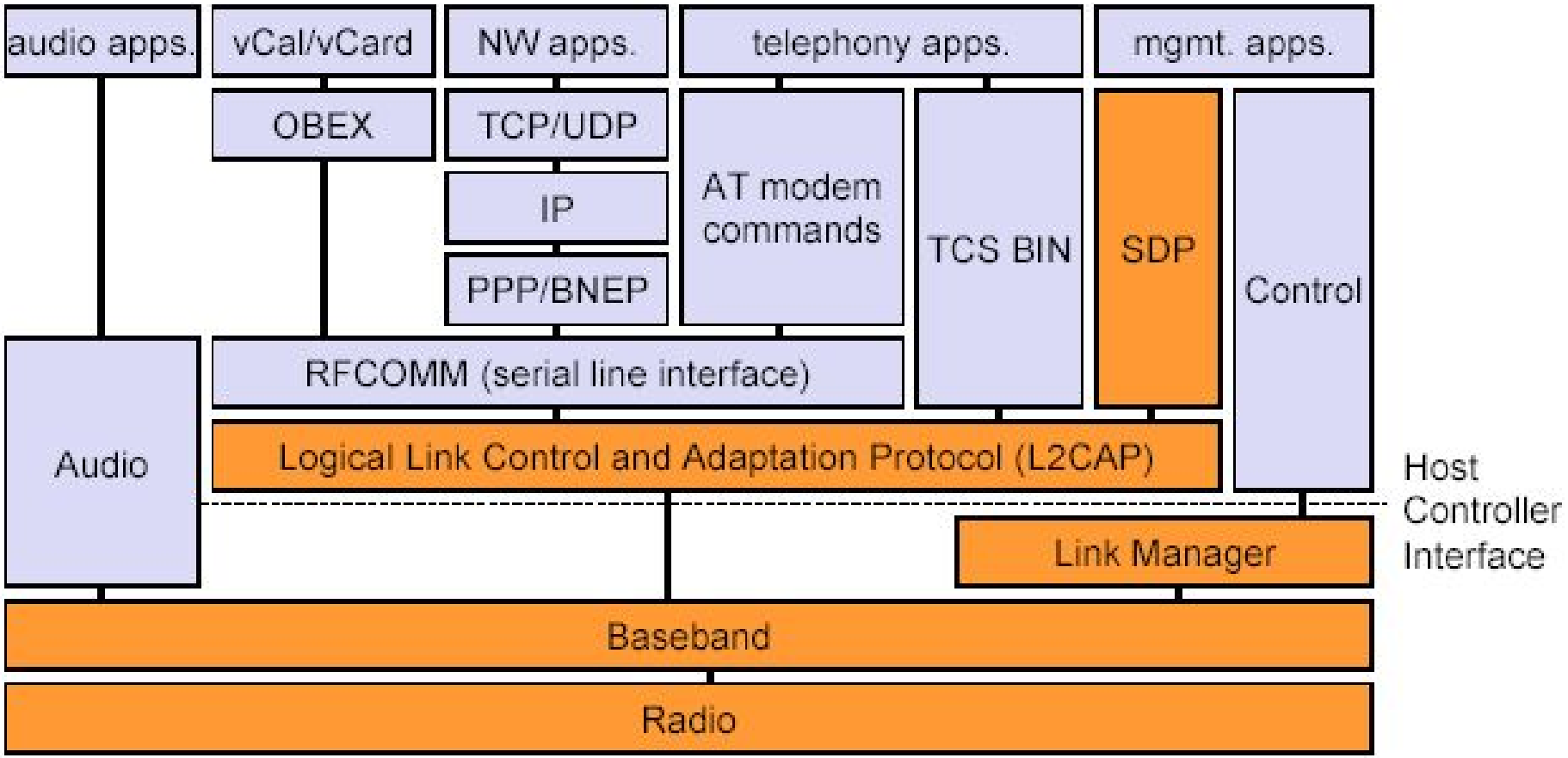


* 2002:
  - pris ~30kr

* 2005:
  - estimert: 670 mil. enheter verden rundt

THALES

Stack'en



AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol

SDP: service discovery protocol
RFCOMM: radio frequency comm.

THALES

Sikkerhet

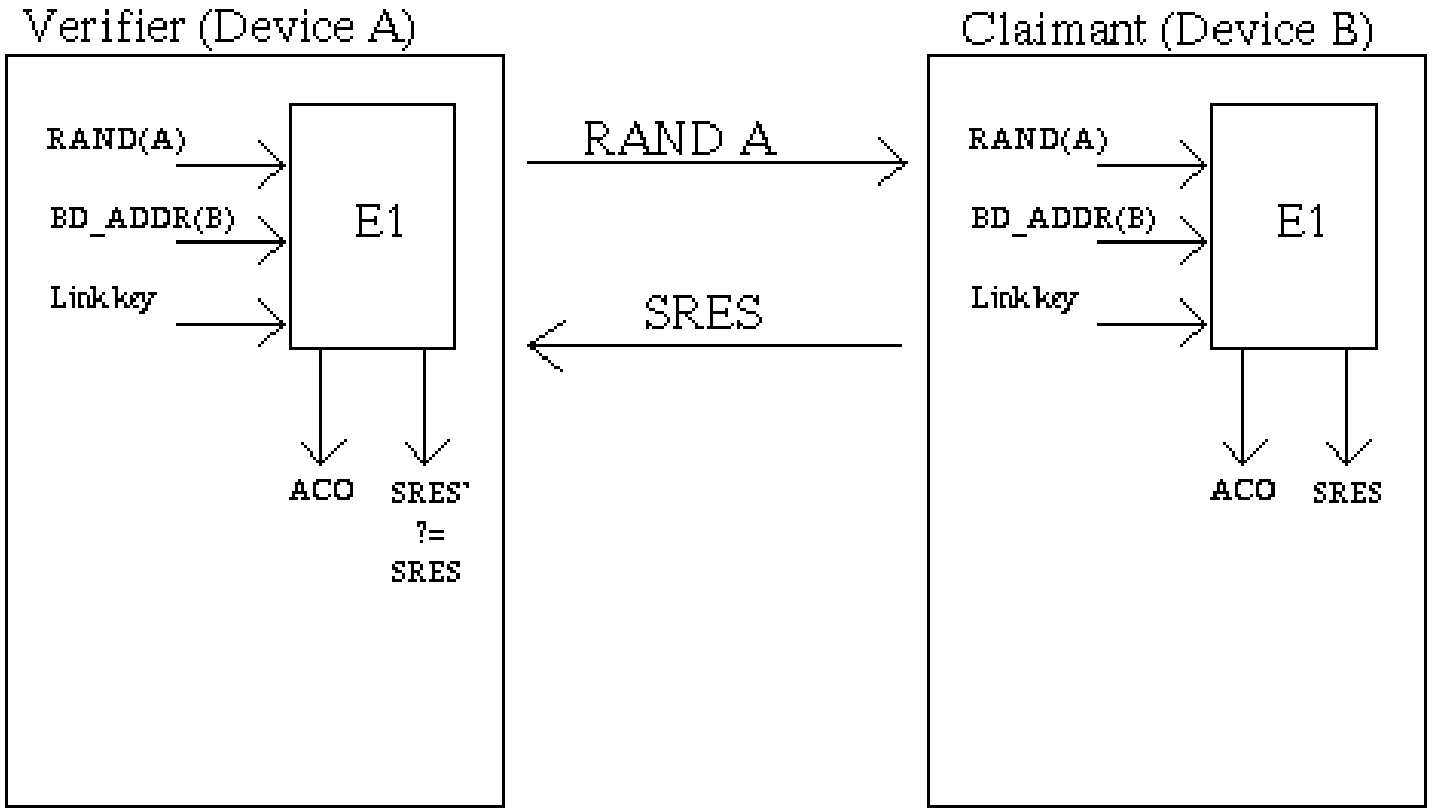
* **bruker fire entiteter for sikkerhet på link nivå:**
  1. **blåtann enhet addresse (BG_ADDR) – 48bit**
  2. **privat autentiseringsnøkkel - tilfeldig 128bit tall**
  3. **private krypteringsnøkkel - 8-128bit**
  4. **ett tilfeldig tall (RAND) – stadig skiftende 128bit**

* **Tre sikkerhetsmodus:**
  1. **usikker**
  2. **tjenestenivå sikkerhet**
     - ulik tilgang til applikasjoner med ulike krav
  3. **linknivå sikkerhet**
     - likt sikkerhetsnivå for alle applikasjoner/enheter
     - enklere å implementere

Autentisering

"vet mottaker den hemmlige nøkkel?"

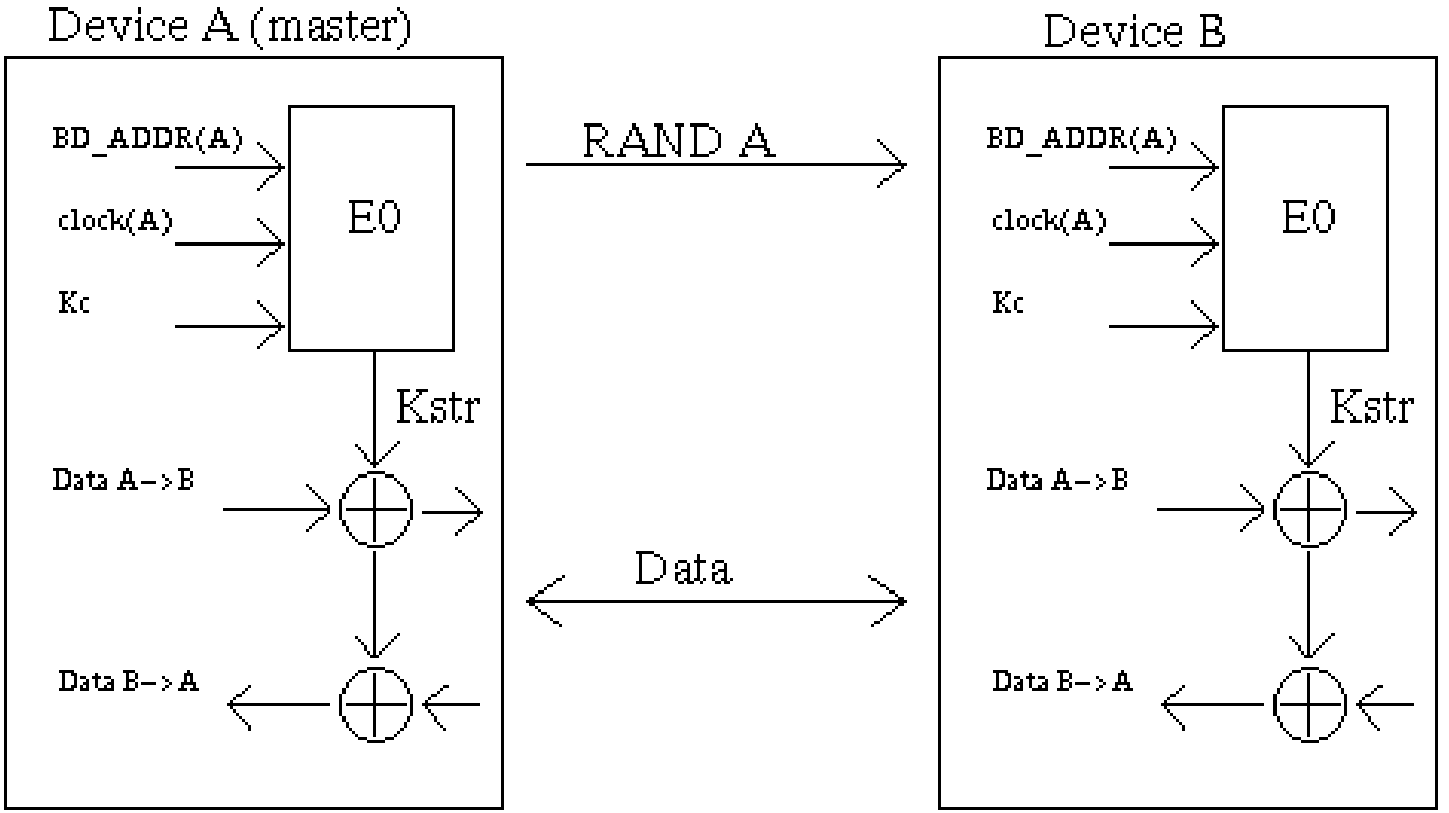
* symmetrisk kryptering, må dele nøkkel
* authentication Ciphering Offeset (ACO) blir brukt til generering av cipher nøkkel senere



THALES

Kryptering

* **krypterer payloaden vha. stream chiper E0:**
  - payload key generator, key stream generator, encryption/decryption generator
* **ulik kryptering i ulike sikkerhetsmodus (nøkkeltype)**
* **nøkkellengde forhandles frem**

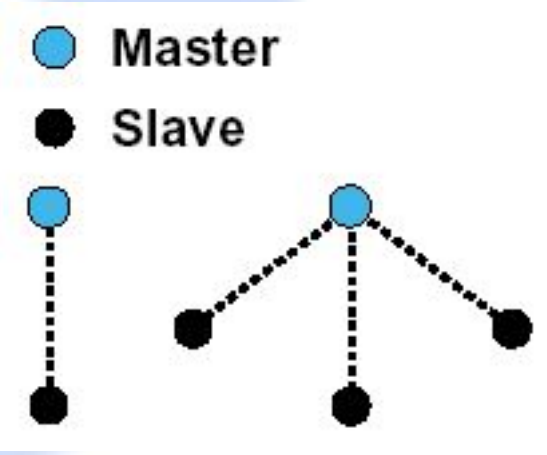


THALES

Piconet:

- Et PAN(personal area network) av BTenheter
- Point-to-point eller point-to-multipoint
- 1 master og opp til 7 slaver
- Slaver følger masters sync i frekvenshoppingen
- Master sender på par og slaver på odde time-slots
-All trafikk foregår via master

Master synkroniserer frekvenshopping og allokerer timeslots for slaver



THALES

Kommunikasjon – to typer forbindelser:

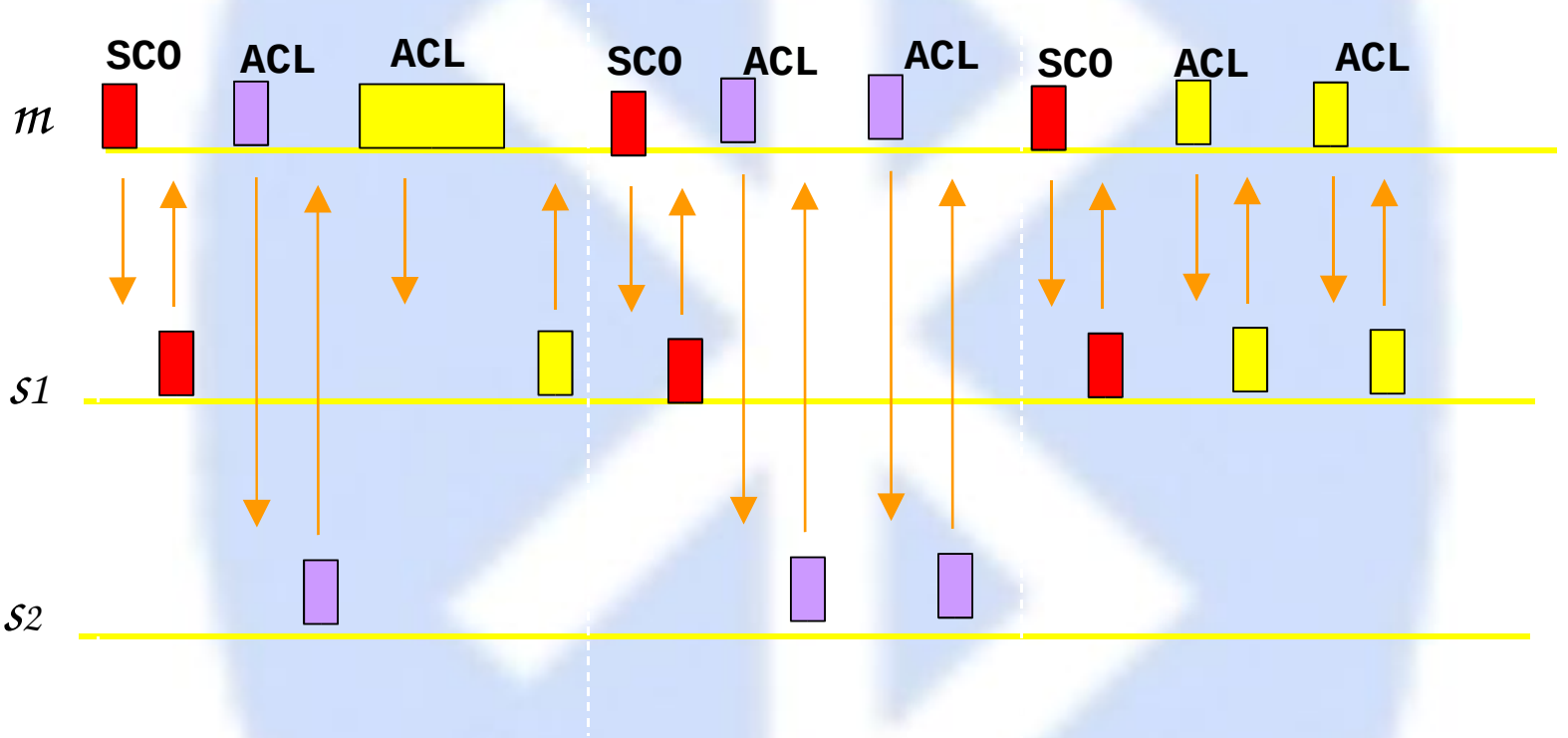
SCO – synchronous connection oriented:

- point-to-point, mellom master og slave
- Reserverer time-slots
- En master kan kjøre 3 samtidige SCO linker
- Passer for tids-kritiske operasjoner
- 64Kbps symmetrisk

ACL – asynchronous conectionless:

- point-to-point eller point-to-multipoint
- Kan kun finnes en ACL link mellom en master og slave
- Slaven kan kun sende på forespørsel fra master
- Symmetrisk 108-433 Kbps, asymmetrisk <723 Kbps

Eksempel på trafikk:

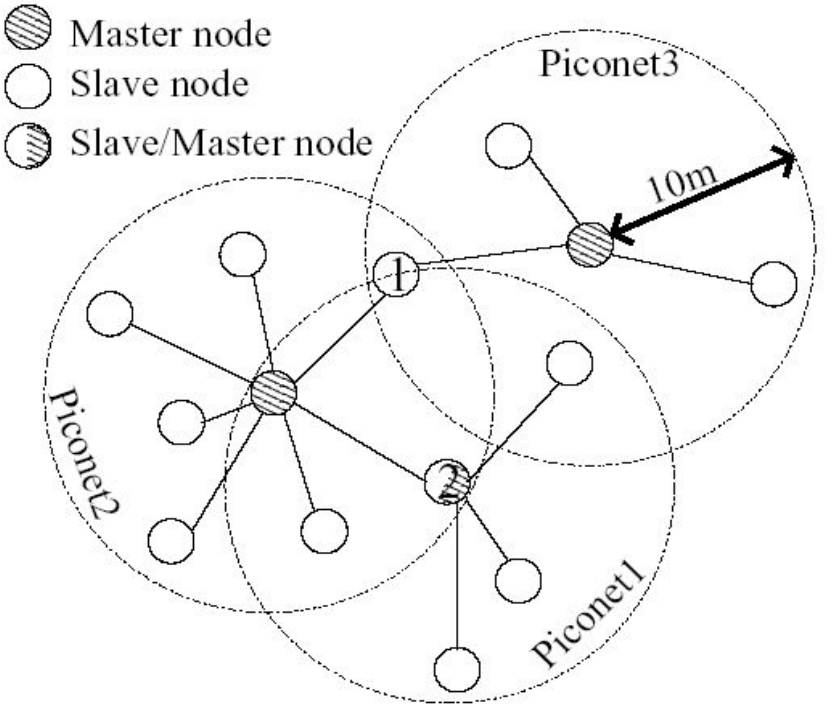


THALES

Scatternet:

- Flere piconet kan danne et *scatternet*
- En master kan være en slave i et annet piconet- Piconets har forskjellige frekvensmønstre
- En node som er medlem i to piconets må multiplexe mellom frekvensmønstrene

Bluetooth *åpner for* kommunikasjon mellom piconets – men det er også alt!



THALES

Scatternet – virkeligheten:

- Forskningsområde
- Ingen definert standard ennå
- Lite detaljer i bluetooth spesifikasjonen
- Støttes ikke av BT-enheter
- Til nå eksisterer ingen virkelige piconets – resultater er basert på simuleringer

Scatternet er teori!

Scatternet som et MANET:

-Foreslåtte ruting-/konfigurasjonsprotokoller:
  - LMS
  - BTCP

-En reaktiv tilnærming er nok å foretrekke for å kunne la BT dra nytte av *standby*

-Overheaden ved transmisjon mellom piconets vil bli stor

-Overhead ved innmelding i nytt piconet

Hvor vil scatternet kunne fungere som MANET?

Hovedkriteriene blir:

- statisk topologi
- reaktiv routing

Med en rekkevidde på 10m(BT 1.0) vil bare en liten grad av fysisk mobilitet i nettet føre til store topologiendringer! Overheaden mellom piconets vil føre til en stor belastning i nettet ved bruk av en proaktiv tilnær ming.

I et statisk “sensornett”, altså med lav grad av mobilitet, vil scatternet kunne fungere som MANET med en reaktiv tilnær ming. Men overheaden ved kommunikasjon vil fremdeles bli stor.

Wireless Personal Area Networks IEEE 802.15

Mål:
to publish standards, recommended practices, or guides that have broad market applicability and deal effectively with the issues of coexistence and interoperability with other wired and wireless networking solutions

Bluetooth og IEEE802.15:
802.15 arbeidsgruppe 1 jobber med bluetooth

I mars 2002 kom IEEE802.15.1 standarden

The approved IEEE 802.15.1 standard is fully compatible with the Bluetooth v1.1

Bluetooth vs. WLAN:

Hvorfor ikke lage en PAN med 802.11?
Sette ned effekten for å begrense rekkevidde og strøm?

	PAN (Bluetooth)	WLAN
Rekkevidde	10-100m	100m
Hastighet	1-2 Mbps	<54Mbps
Sikkerhet	Ja	WEP, IPSec +++
Ant. noder	8	Mange
Multihopp	Begrenset	Omfattende med ad-hoc
Oppsett	**Enkelt**	Ikke så enkelt (wep/IP)
pris/str	**Billig/liten**	Ikke så billig/større
Frekvenshopp	Ja	Ja