Course 132

Technical Introduction to CDMA

IS-95 CDMA *and a few details of CDMA2000 1x*

Course Outline

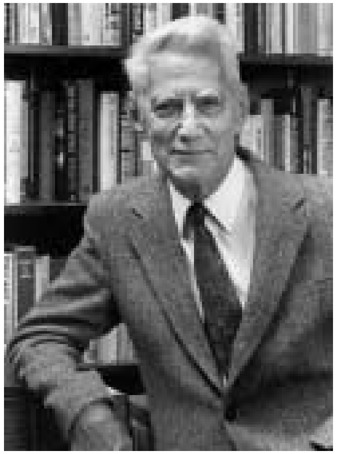
- Basic CDMA Principles
  - Coding
  - Forward and Reverse Channels
- CDMA Operational Details
  - Multiplexing, Forward and Reverse Power Control
- CDMA Handset Architecture
- CDMA Handoffs
- CDMA Network Architecture
- CDMA Messaging and Call Flow
- Optional Topics
- Wireless Multiple Access Technologies
- Overview of Current Technologies
  - Capacity; CDMA Overlays, Spectrum Clearing

Section A

How Does CDMA Work?
Introduction to Basic Principles

Claude Shannon:
The Einstein of Information Theory

- The core idea that makes CDMA possible was first explained by Claude Shannon, a Bell Labs research mathematician
- Shannon's work relates amount of information carried, channel bandwidth, signal-to-noise-ratio, and detection error probability
    - It shows the theoretical upper limit attainable



In 1948 **Claude Shannon** published his landmark paper on information theory, ***A Mathematical Theory of Communication***. He observed that "the fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point." His paper so clearly established the foundations of information theory that his framework and terminology are standard today. Shannon died Feb. 24, 2001, at age 84.

SHANNON'S CAPACITY EQUATION

$$\mathbf{C = B_{\omega} \log_2 \left[1 + \frac{S}{N} \right]}$$

B_{ω} = bandwidth in Hertz
C = channel capacity in bits/second
S = signal power
N = noise power

CDMA: Using A New Dimension

- All CDMA users occupy the same frequency at the same time! Frequency and time are not used as discriminators
- CDMA operates by using CODING to discriminate between users
- CDMA interference comes mainly from nearby users
- Each user is a small voice in a roaring crowd -- but with a uniquely recoverable code

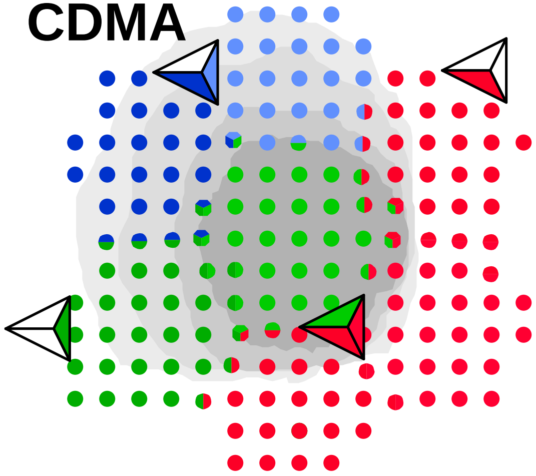
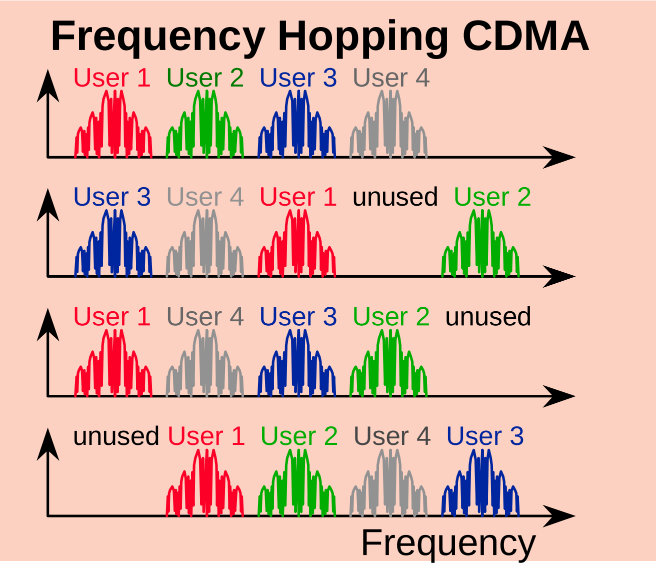
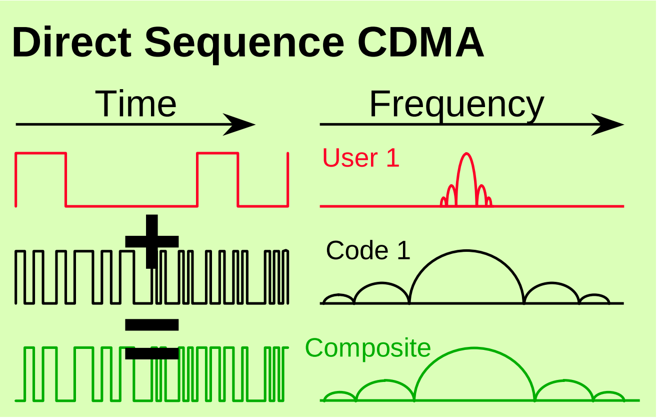


Figure of Merit: C/I
(carrier/interference ratio)
AMPS: +17 dB
TDMA: +14 to +17 dB
GSM: +7 to 9 dB.
CDMA: -10 to -17 dB.
CDMA: E_b/N_o ~+6 dB.

Two Types of CDMA





There are Two types of CDMA:

- **Frequency-Hopping**
  - Each user’s narrowband signal hops among discrete frequencies, and the receiver follows in sequence
  - **Frequency-Hopping Spread Spectrum (FHSS)** CDMA is **NOT** currently used in wireless systems, although used by the military
- **Direct Sequence**
  - narrowband input from a user is coded (“spread”) by a user-unique broadband code, then transmitted
  - broadband signal is received; receiver knows, applies user’s code, recovers users’ data
  - **Direct Sequence Spread Spectrum (DSSS)** CDMA **IS** the method used in IS-95 commercial systems

DSSS Spreading: Time-Domain View

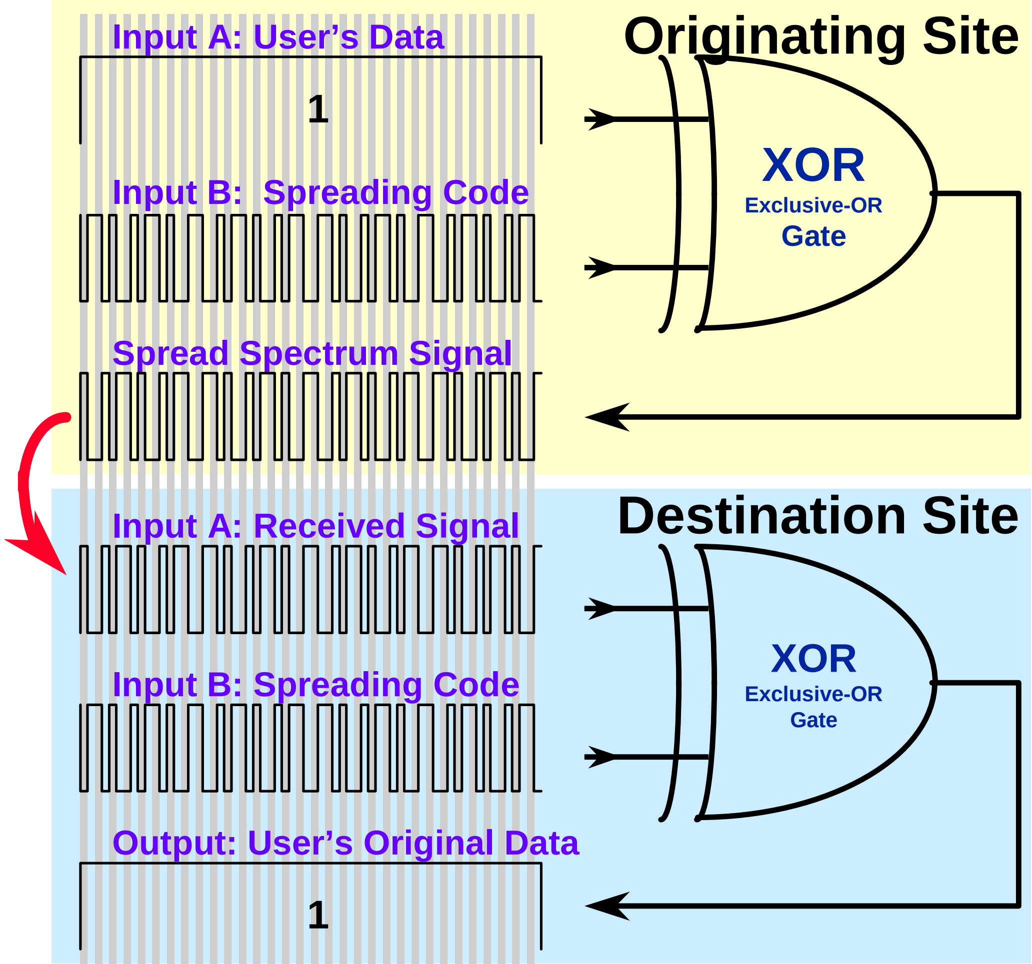
At Originating Site:

- Input A: User's Data @ 19,200 bits/second
- Input B: Walsh Code #23 @ 1.2288 Mcps
- Output: Spread spectrum signal

via air interface

At Destination Site:

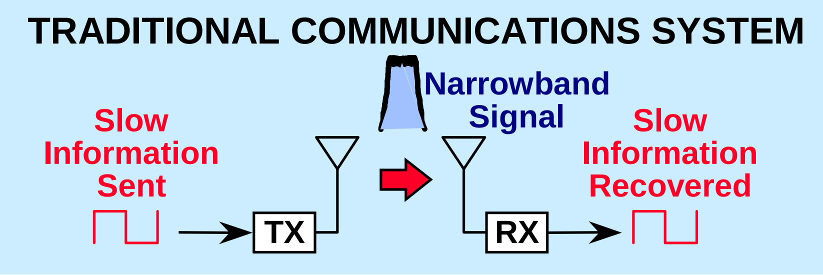
- Input A: Received spread spectrum signal
- Input B: Walsh Code #23 @ 1.2288 Mcps
- Output: User's Data @ 19,200 bits/second just as originally sent

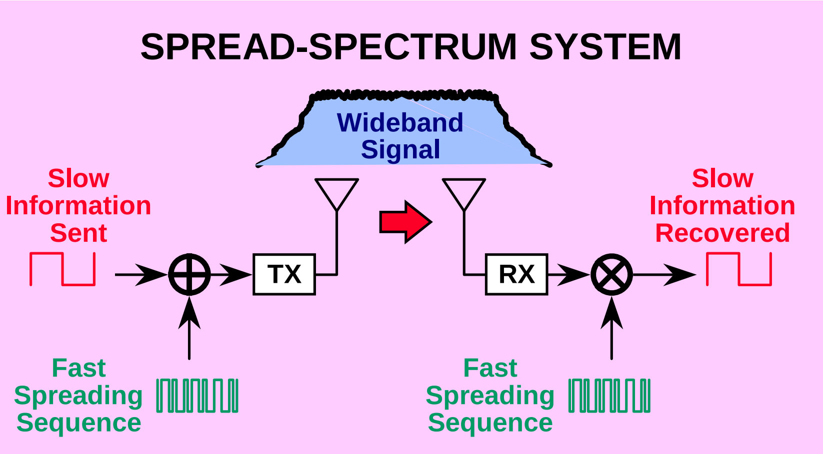


Drawn to actual scale and time alignment

Spreading from a Frequency-Domain View

- Traditional technologies try to squeeze signal into minimum required bandwidth
- CDMA uses larger bandwidth but uses resulting processing gain to increase capacity





Spread Spectrum Payoff:
Processing Gain

The CDMA Spread Spectrum Payoff:
Would you like a lump-sum, or monthly payments?

- Shannon's work suggests that a certain bit rate of information deserves a certain bandwidth
- If one CDMA user is carried alone by a CDMA signal, the processing gain is large - roughly 21 db for an 8k vocoder.
  - Each doubling of the number of users consumes 3 db of the processing gain
  - Somewhere above 32 users, the signal-to-noise ratio becomes undesirable and the ultimate capacity of the sector is reached
- Practical CDMA systems restrict the number of users per sector to ensure processing gain remains at usable levels

CDMA Spreading Gain

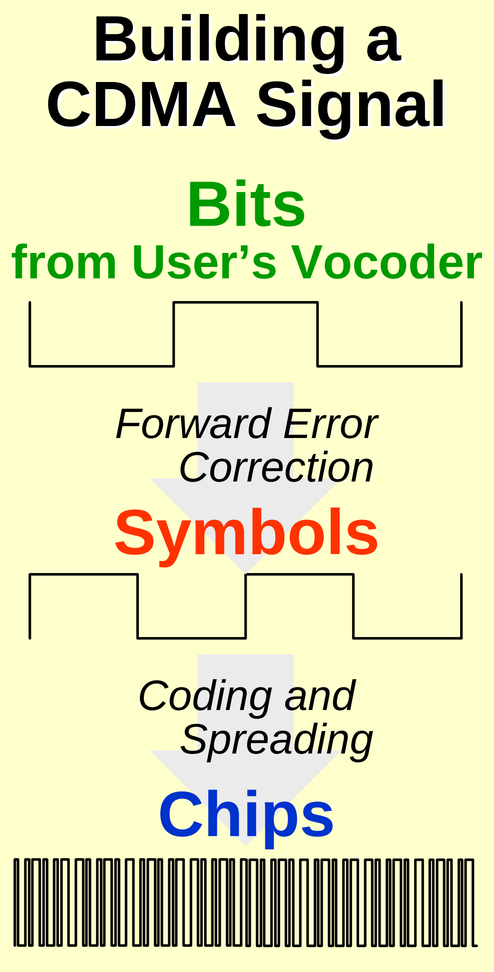
Consider a user with a 9600 bps vocoder talking on a CDMA signal 1,228,800 hz wide. The processing gain is 1,228,800/9600 = 128, which is 21 db. What happens if additional users are added?

# Users	Processing Gain
1	21 db
2	18 db
4	15 db
8	12 db
16	9 db
32	6 db

64…..Uh, Regis, can I just take the money I've already won, and go home now?

CDMA Uses Code Channels

- A CDMA signal uses many chips to convey just one bit of information
- Each user has a unique chip pattern, in effect a code channel
- To recover a bit, integrate a large number of chips interpreted by the user's known code pattern
- Other users' code patterns appear random and integrate in a random self-canceling fashion, don't disturb the bit decoding decision being made with the proper code pattern



Building a CDMA Signal

Bits

from User's Vocoder

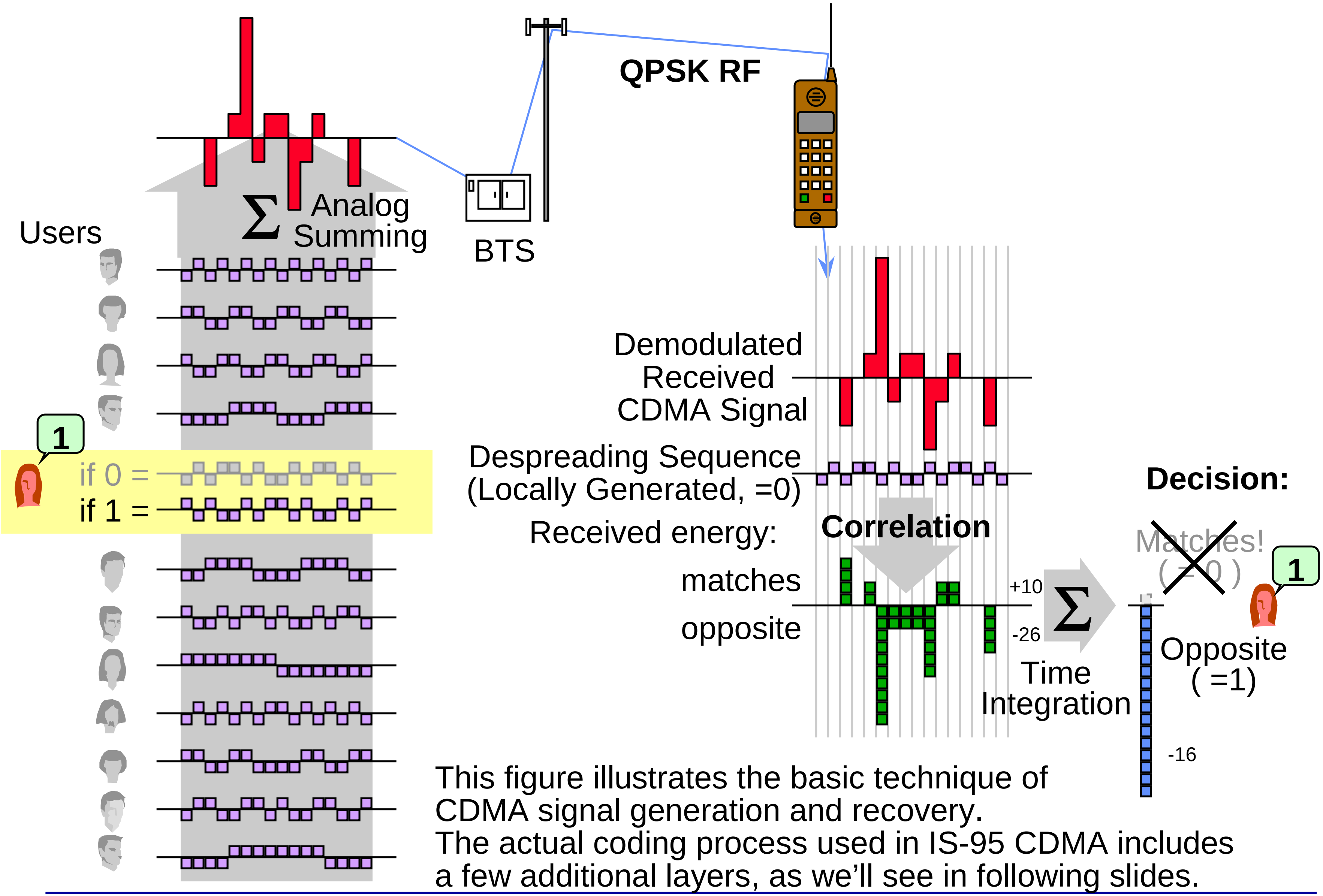
Forward Error Correction

Symbols

Coding and Spreading

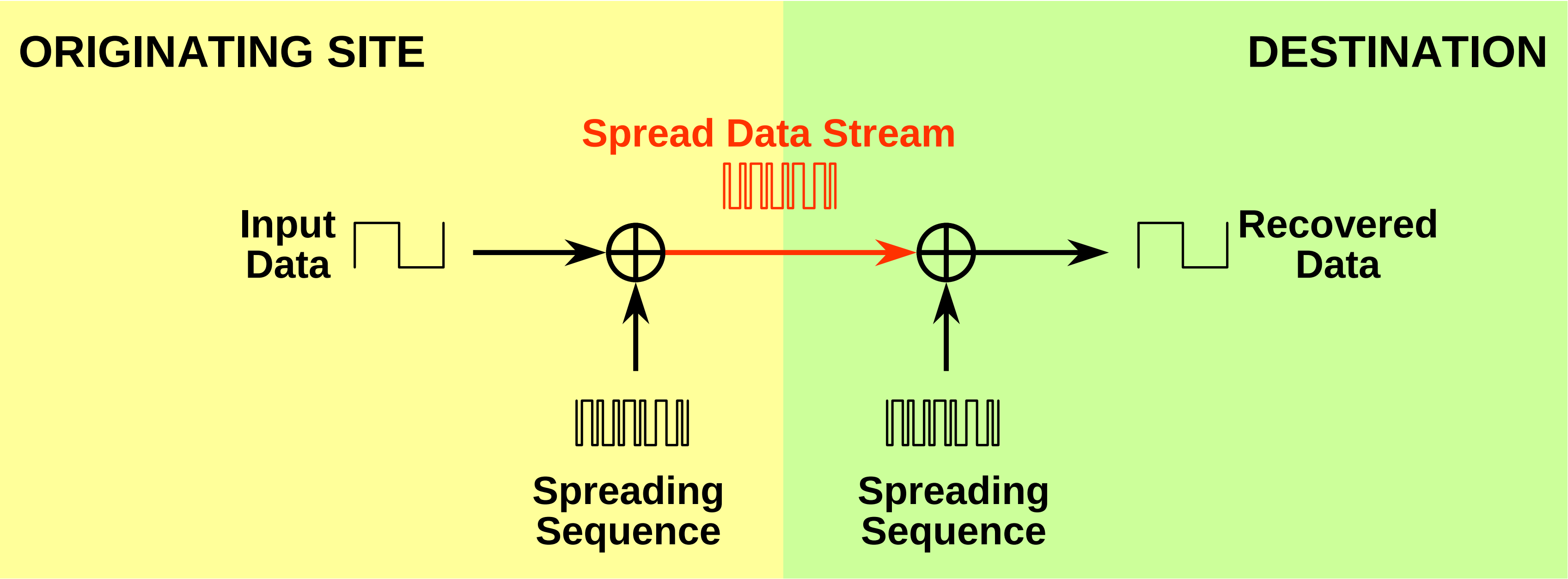
Chips

How a BTS Sector Serves Multiple Users



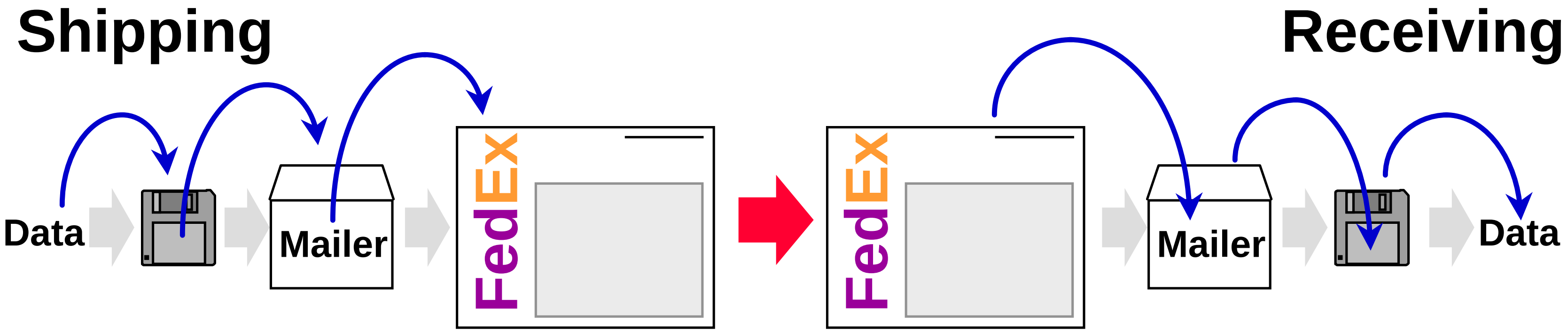
This figure illustrates the basic technique of CDMA signal generation and recovery.
The actual coding process used in IS-95 CDMA includes a few additional layers, as we'll see in following slides.

Spreading: What we do, we can undo



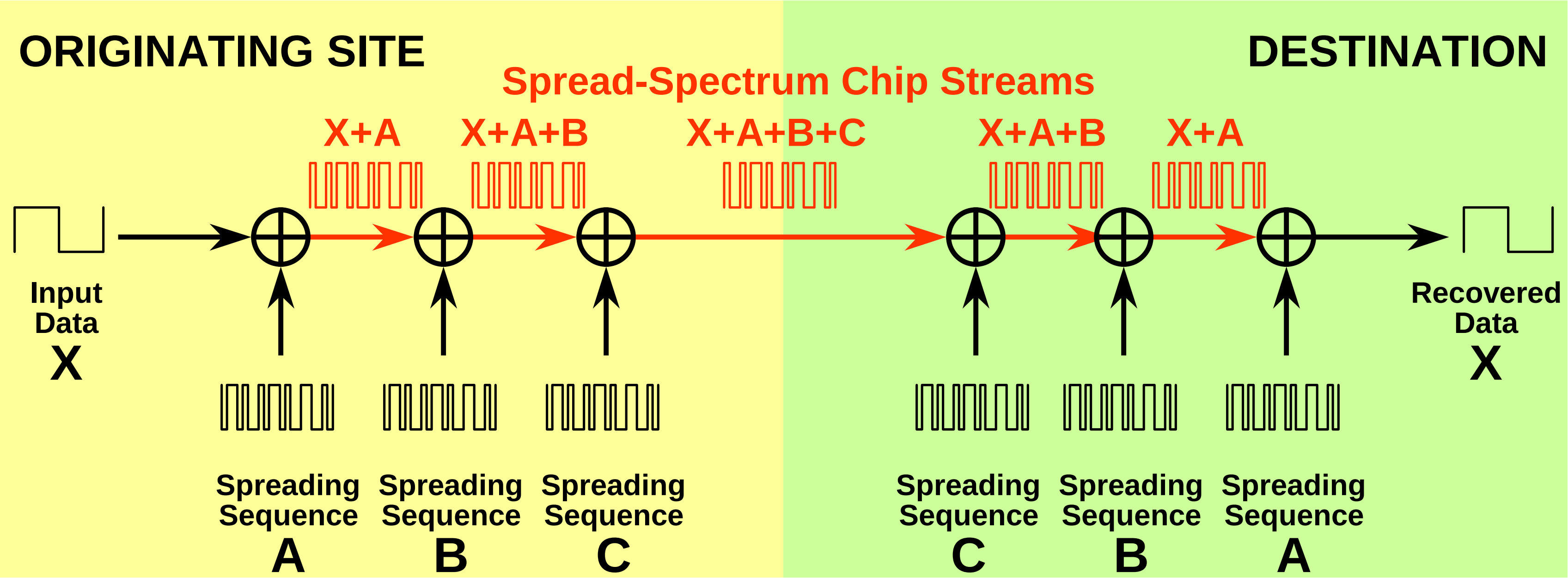
- Sender combines data with a fast spreading sequence, transmits spread data stream
- Receiver intercepts the stream, uses same spreading sequence to extract original data

"Shipping and Receiving" via CDMA



- Whether in shipping and receiving, or in CDMA, packaging is extremely important!
- Cargo is placed inside "nested" containers for protection and to allow addressing
- The shipper packs in a certain order, and the receiver unpacks in the reverse order
- CDMA "containers" are spreading codes

CDMA's Nested Spreading Sequences



- CDMA combines three different spreading sequences to create unique, robust channels
- The sequences are easy to generate on both sending and receiving ends of each link
- "What we do, we can undo"

One of the CDMA Spreading Sequences: Walsh Codes

- 64 “Magic” Sequences, each 64 chips long
- Each Walsh Code is precisely Orthogonal with respect to all other Walsh Codes
  - it’s simple to generate the codes, or
  - they’re small enough to use from ROM

Unique Properties:

Mutual Orthogonality

EXAMPLE:

Correlation of Walsh Code #23 with Walsh Code #59

```
#23   0110100101101001100101101001011001101001011010011001011010010110
#59   0110011010011001100110010110011010011001011001100110011010011001
Sum   0000111111110000000011111111000011110000000011111111000000001111
```

Correlation Results: 32 1’s, 32 0’s: Orthogonal!!

WALSH CODES

#	------------------------------ 64-Chip Sequence ------------------------------
0	0000000000000000000000000000000000000000000000000000000000000000
1	0101010101010101010101010101010101010101010101010101010101010101
2	0011001100110011001100110011001100110011001100110011001100110011
3	0110011001100110011001100110011001100110011001100110011001100110
4	0000111100001111000011110000111100001111000011110000111100001111
5	0101101001011010010110100101101001011010010110100101101001011010
6	0011110000111100001111000011110000111100001111000011110000111100
7	0110100101101001011010010110100101101001011010010110100101101001
8	0000000011111111000000001111111100000000111111110000000011111111
9	0101010110101010010101011010101001010101101010100101010110101010
10	0011001111001100001100111100110000110011110011000011001111001100
11	0110011010011001011001101001100101100110100110010110011010011001
12	0000111111110000000011111111000000001111111100000000111111110000
13	0101101010100101010110101010010101011010101001010101101010100101
14	0011110011000011001111001100001100111100110000110011110011000011
15	0110100110010110011010011001011001101001100101100110100110010110
16	0000000000000000111111111111111100000000000000001111111111111111
17	0101010101010101101010101010101001010101010101011010101010101010
18	0011001100110011110011001100110000110011001100111100110011001100
19	0110011001100110100110011001100101100110011001101001100110011001
20	0000111100001111111100001111000000001111000011111111000011110000
21	0101101001011010101001011010010101011010010110101010010110100101
22	0011110000111100110000111100001100111100001111001100001111000011
23	0110100101101001100101101001011001101001011010011001011010010110
24	0000000011111111111111110000000000000000111111111111111100000000
25	0101010110101010101010100101010101010101101010101010101001010101
26	0011001111001100110011000011001100110011110011001100110000110011
27	0110011010011001100110010110011001100110100110011001100101100110
28	0000111111110000111100000000111100001111111100001111000000001111
29	0101101010100101101001010101101001011010101001011010010101011010
30	0011110011000011110000110011110000111100110000111100001100111100
31	0110100110010110100101100110100101101001100101101001011001101001
32	0000000000000000000000000000000011111111111111111111111111111111
33	0101010101010101010101010101010110101010101010101010101010101010
34	0011001100110011001100110011001111001100110011001100110011001100
35	0110011001100110011001100110011010011001100110011001100110011001
36	0000111100001111000011110000111111110000111100001111000011110000
37	0101101001011010010110100101101010100101101001011010010110100101
38	0011110000111100001111000011110011000011110000111100001111000011
39	0110100101101001011010010110100110010110100101101001011010010110
40	0000000011111111000000001111111111111111000000001111111100000000
41	0101010110101010010101011010101010101010010101011010101001010101
42	0011001111001100001100111100110011001100001100111100110000110011
43	0110011010011001011001101001100110011001011001101001100101100110
44	0000111111110000000011111111000011110000000011111111000000001111
45	0101101010100101010110101010010110100101010110101010010101011010
46	0011110011000011001111001100001111000011001111001100001100111100
47	0110100110010110011010011001011010010110011010011001011001101001
48	0000000000000000111111111111111111111111111111110000000000000000
49	0101010101010101101010101010101010101010101010100101010101010101
50	0011001100110011110011001100110011001100110011000011001100110011
51	0110011001100110100110011001100110011001100110010110011001100110
52	0000111100001111111100001111000011110000111100000000111100001111
53	0101101001011010101001011010010110100101101001010101101001011010
54	0011110000111100110000111100001111000011110000110011110000111100
55	0110100101101001100101101001011010010110100101100110100101101001
56	0000000011111111111111110000000011111111000000000000000011111111
57	0101010110101010101010100101010110101010010101010101010110101010
58	0011001111001100110011000011001111001100001100110011001111001100
59	0110011010011001100110010110011010011001011001100110011010011001
60	0000111111110000111100000000111111110000000011110000111111110000
61	0101101010100101101001010101101010100101010110100101101010100101
62	0011110011000011110000110011110011000011001111000011110011000011
63	0110100110010110100101100110100110010110011010010110100110010110

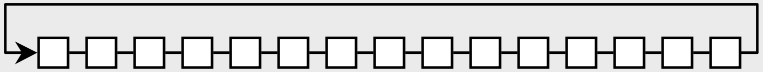
In CDMA2000, user data comes at various speeds, and different lengths of walsh codes can exist.

See Course 332 for more details on CDMA2000 1xRTT fast data channels and additional Walsh codes.

Other Sequences: Generation & Properties

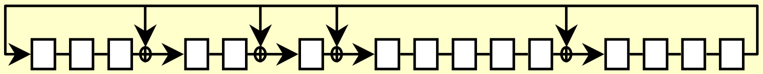
- Other CDMA sequences are generated in shift registers
- Plain shift register: no fun, sequence = length of register
- Tapped shift register generates a wild, self-mutating sequence 2^N-1 chips long (N=register length)
  - Such sequences match if compared in step (no-brainer, any sequence matches itself)
  - Such sequences appear approximately orthogonal if compared with themselves not exactly matched in time
  - false correlation typically <2%

An Ordinary Shift Register



Sequence repeats *every **N** chips*,
where N is number of cells in register

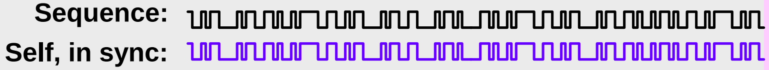
A Tapped, Summing Shift Register



Sequence repeats *every **2^N-1** chips*,
where N is number of cells in register

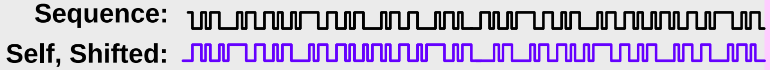
A Special Characteristic of Sequences Generated in Tapped Shift Registers

Compared In-Step: Matches Itself



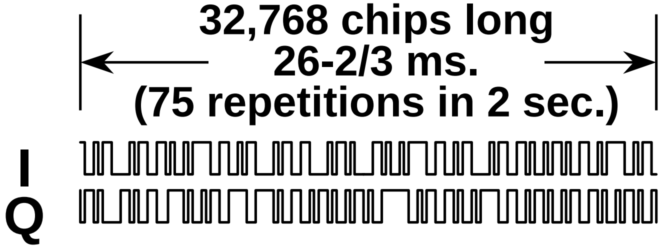
Sum: **Complete Correlation: All 0's**

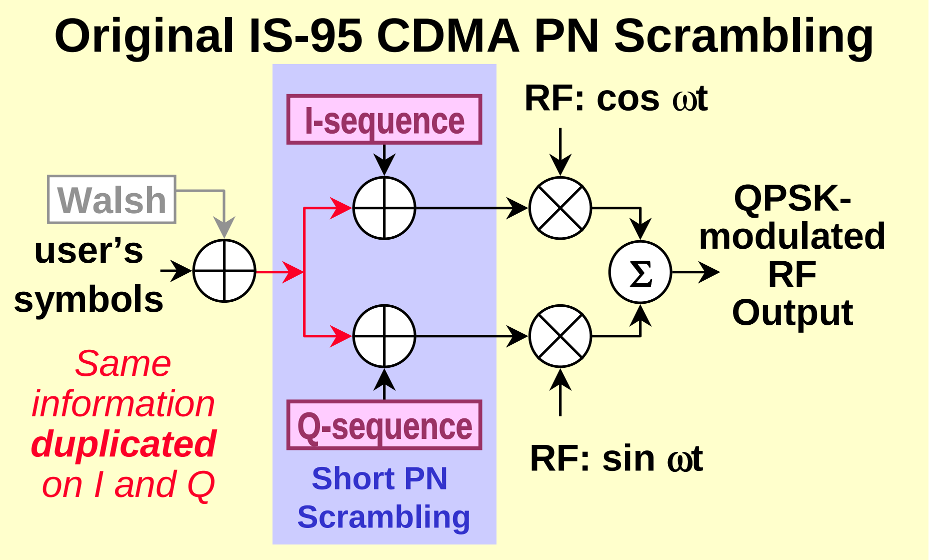
Compared Shifted: Little Correlation

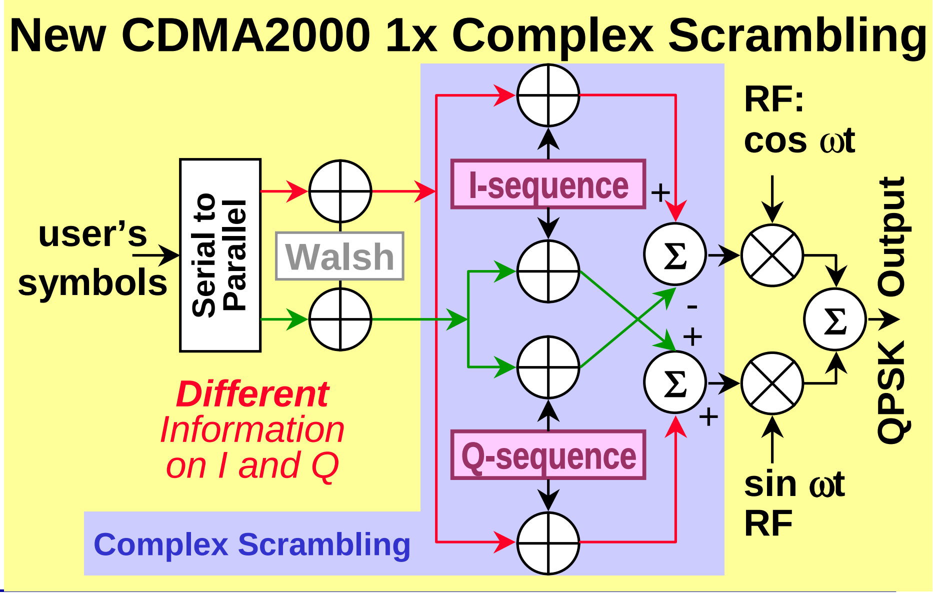


Sum: **Practically Orthogonal: Half 1's, Half 0's**

Another CDMA Spreading Sequence: The Short PN Code, used for Scrambling



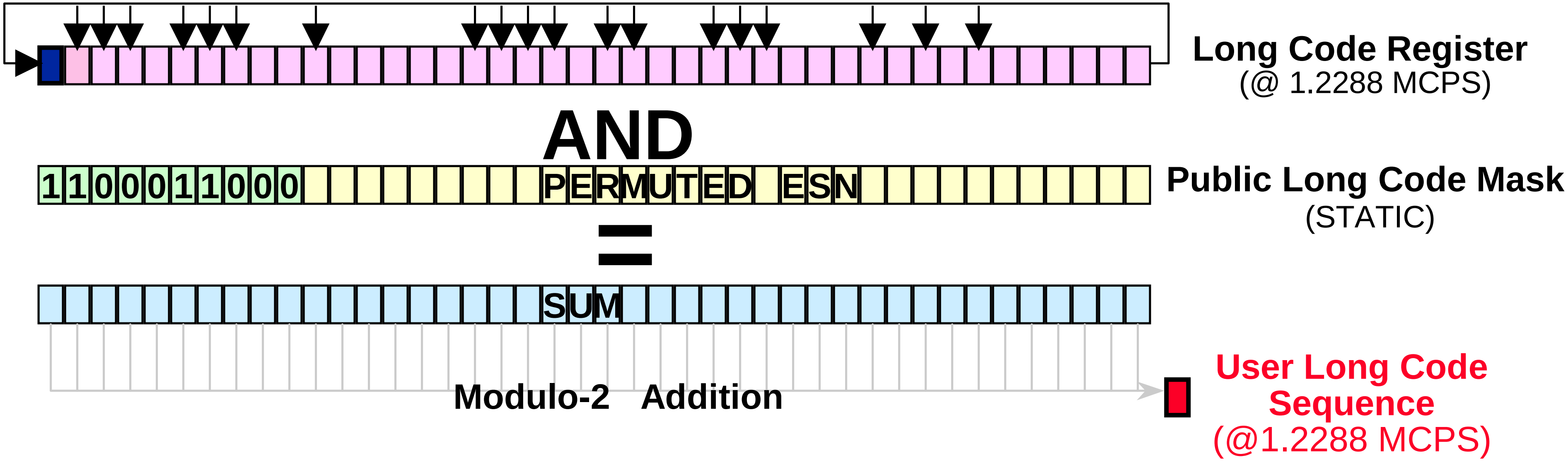




- The short PN code consists of two PN Sequences, I and Q, each 32,768 chips long
  - Generated in similar but differently-tapped 15-bit shift registers
  - the two sequences scramble the information on the I and Q phase channels
- Figures to the right show how one user's channel is built at the bTS

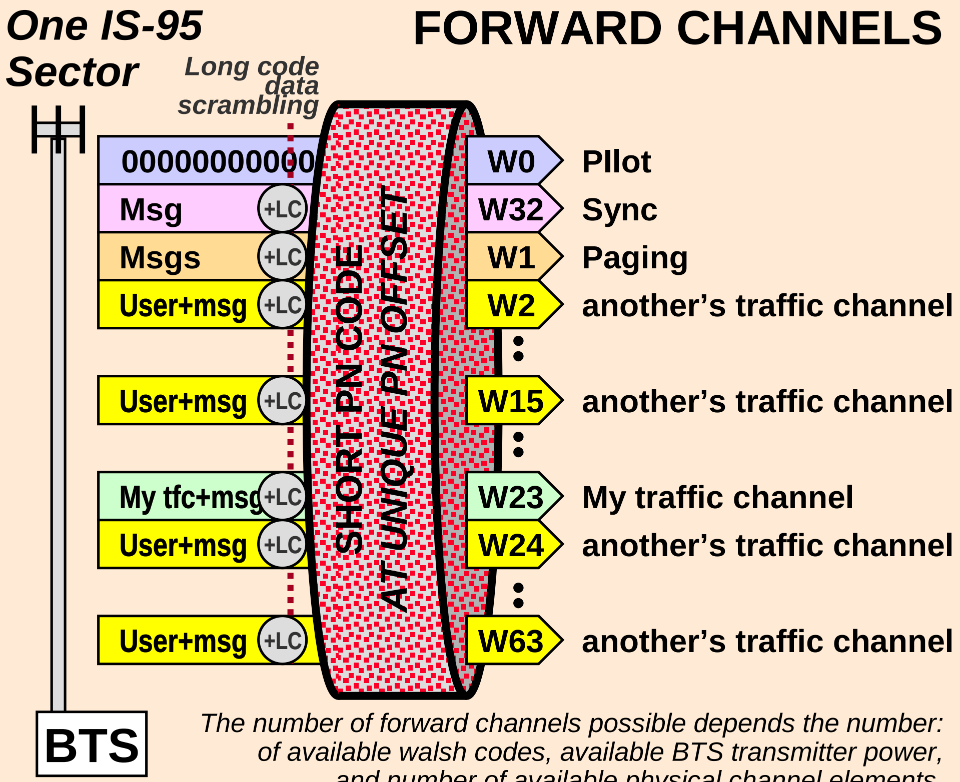
Third CDMA Spreading Sequence: Long Code

Generation & Masking to establish Offset

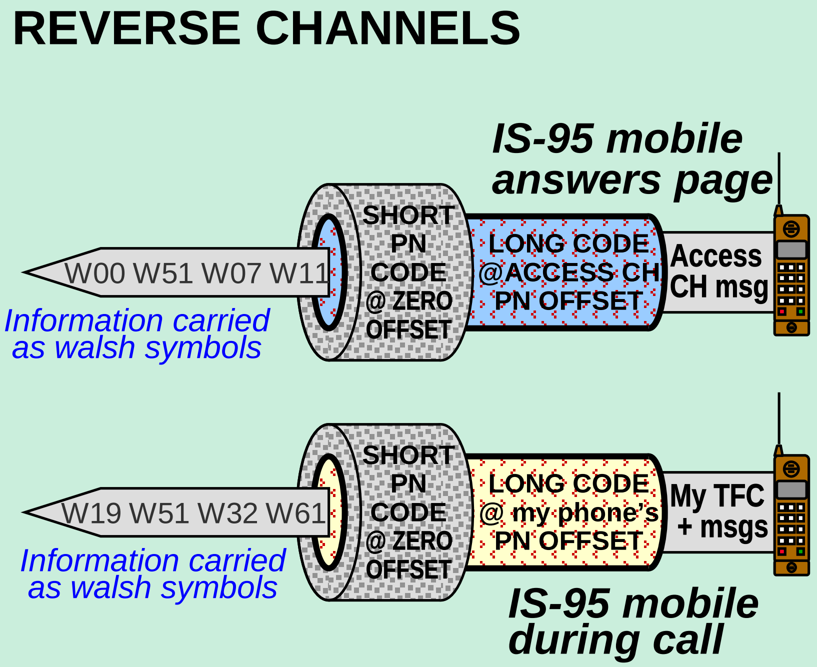


- Generated in a 42-bit register, the PN Long code is more than 40 days long (~4x10^{13} chips) -- too big to store in ROM in a handset, so it's generated chip-by-chip using the scheme shown above
- Each handset codes its signal with the PN Long Code, but at a unique offset computed using its ESN (32 bits) and 10 bits set by the system
  - this is called the "Public Long Code Mask"; produces unique shift
  - private long code masks are available for enhanced privacy
- Integrated over a period even as short as 64 chips, phones with different PN long code offsets will appear practically orthogonal

Summing Up: IS-95 CDMA Channel Makeup



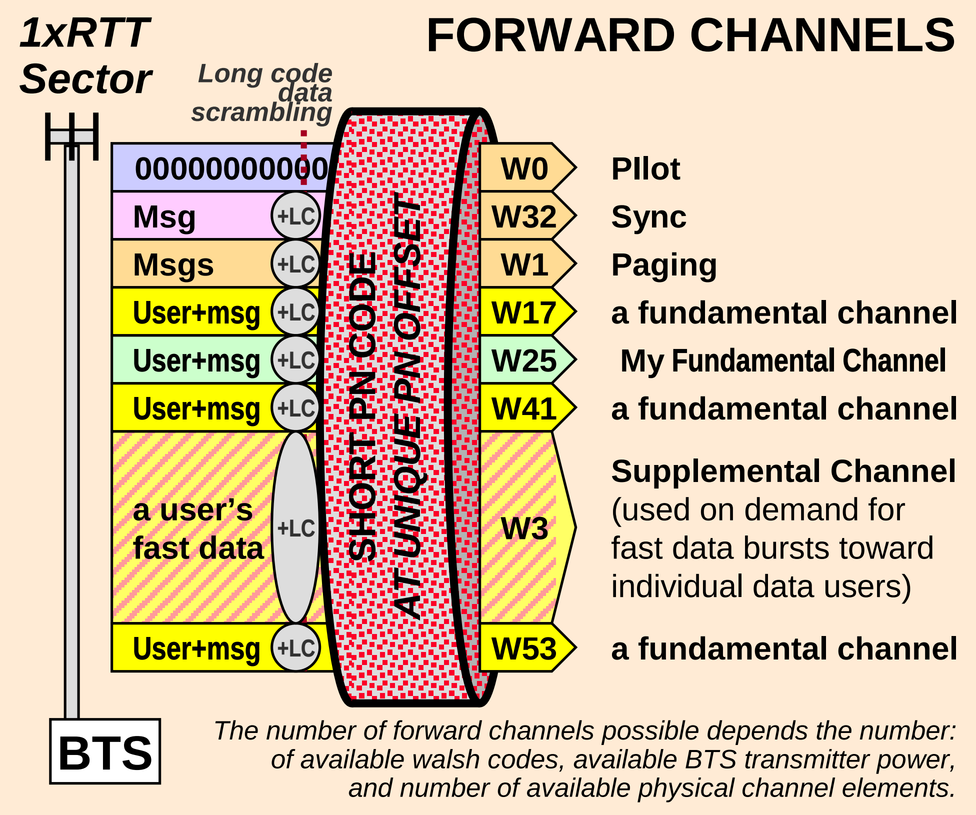
The number of forward channels possible depends the number: of available walsh codes, available BTS transmitter power, and number of available physical channel elements.



Each mobile uses its ESN to determine its own unique Long PN offset. There are at least 2^32 offsets possible, plus additional optional private long code offsets. The limit really depends on S/N.

- THE IS-95 FORWARD LINK
  - each channel is a separate walsh code
  - the short code PN offset makes the sector's signal unique
  - each channel is "data scrambled" with its user's decimated long code
- THE IS-95 REVERSE LINK
  - each mobile has its own unique PN long code offset
  - each mobile uses a walsh code stream to convey its information
  - each mobile uses the Short PN code at 0 offset for QPSK modulation

1xRTT: More Channels, More Capabilities



FORWARD CHANNELS

1xRTT Sector

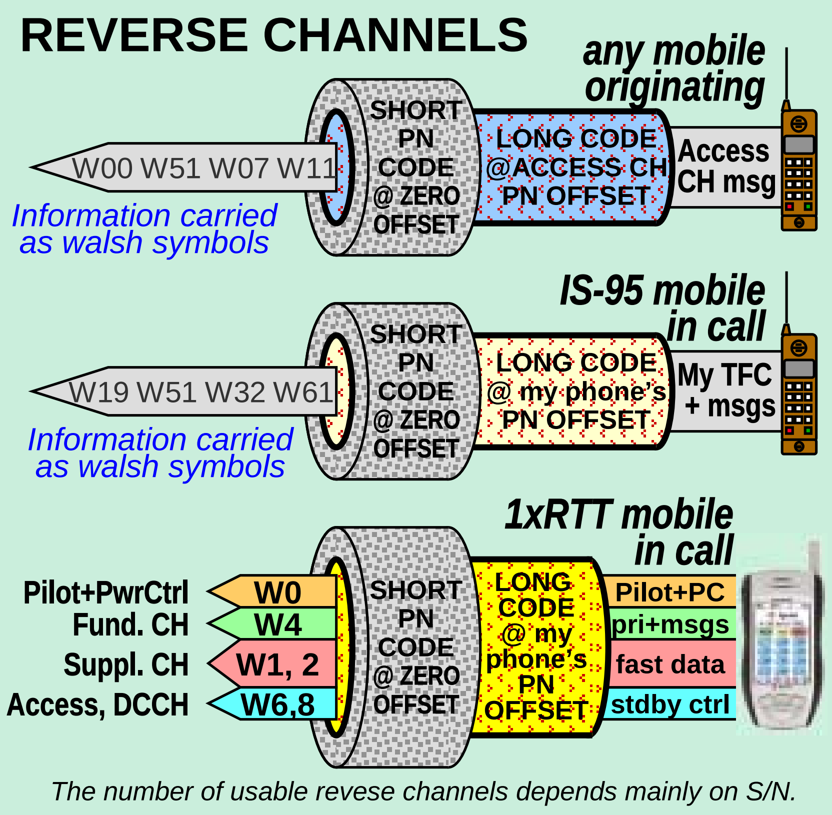
Long code data scrambling

SHORT PN CODE AT UNIQUE PN OFFSET

000000000000		W0	PIlot
Msg	+LC	W32	Sync
Msgs	+LC	W1	Paging
User+msg	+LC	W17	a fundamental channel
User+msg	+LC	W25	My Fundamental Channel
User+msg	+LC	W41	a fundamental channel
a user's fast data	+LC	W3	**Supplemental Channel** (used on demand for fast data bursts toward individual data users)
User+msg	+LC	W53	a fundamental channel

BTS

The number of forward channels possible depends the number: of available walsh codes, available BTS transmitter power, and number of available physical channel elements.



REVERSE CHANNELS

any mobile originating

W00 W51 W07 W11 — SHORT PN CODE @ ZERO OFFSET — LONG CODE @ACCESS CH PN OFFSET — Access CH msg

Information carried as walsh symbols

IS-95 mobile in call

W19 W51 W32 W61 — SHORT PN CODE @ ZERO OFFSET — LONG CODE @ my phone's PN OFFSET — My TFC + msgs

Information carried as walsh symbols

1xRTT mobile in call

SHORT PN CODE @ ZERO OFFSET — LONG CODE @ my phone's PN OFFSET

Pilot+PwrCtrl	W0	Pilot+PC
Fund. CH	W4	pri+msgs
Suppl. CH	W1, 2	fast data
Access, DCCH	W6,8	stdby ctrl

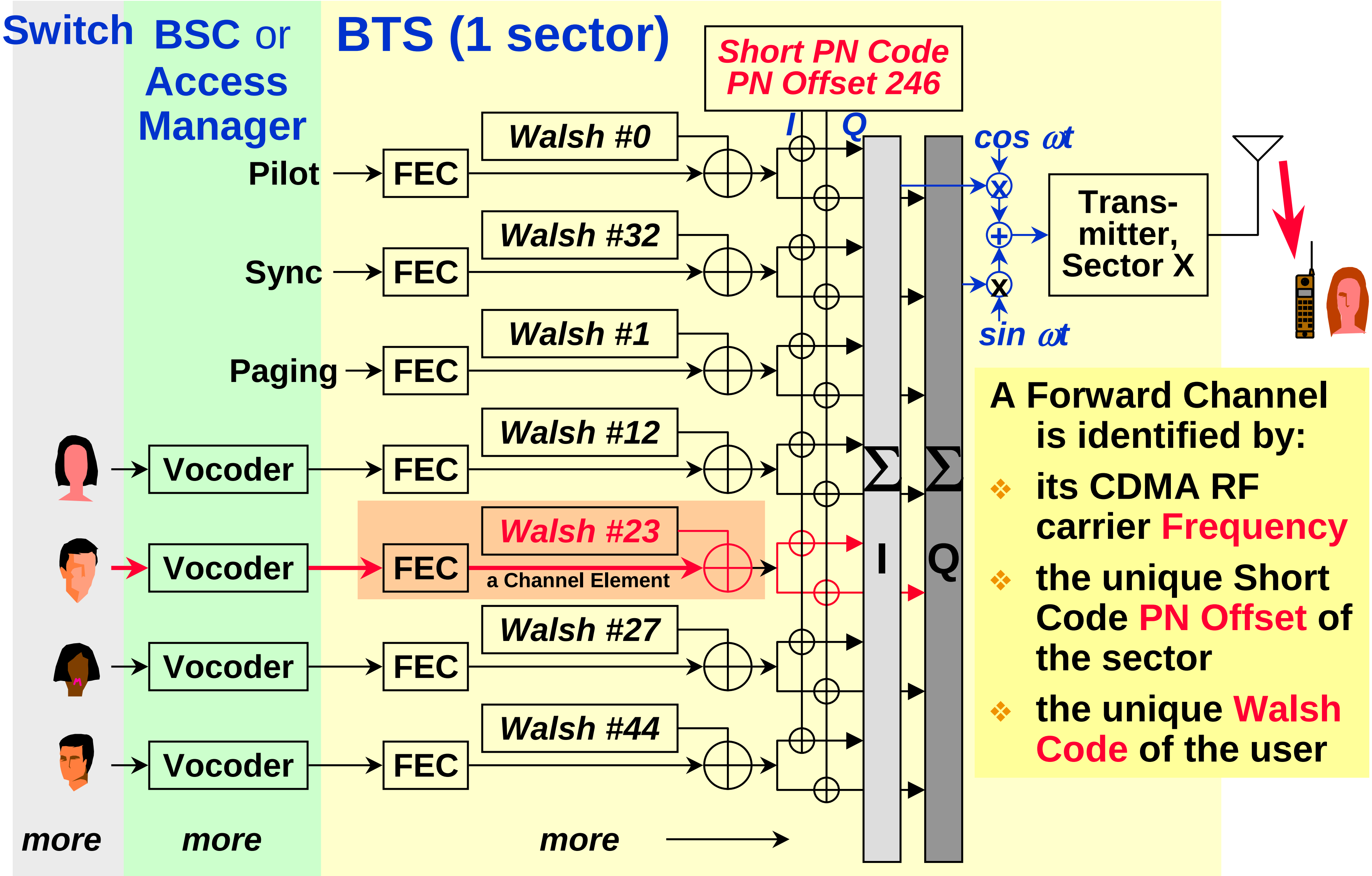
The number of usable revese channels depends mainly on S/N.

- THE 1xRTT FORWARD LINK
  - ***independent I and Q** information content*
  - **different length walsh codes carry channels of different speeds**
  - the short code PN offset makes the sector's signal unique
  - each channel is "data scrambled" with its user's decimated long code
- THE 1xRTT REVERSE LINK
  - ***Independent I and Q** information content*
  - each mobile has its own unique PN long code offset
  - ***each mobile uses separate steady walsh codes for various reverse channels***
  - each mobile uses the Short PN code at 0 offset for QPSK modulation

Section B

IS-95 CDMA Forward and Reverse Channels

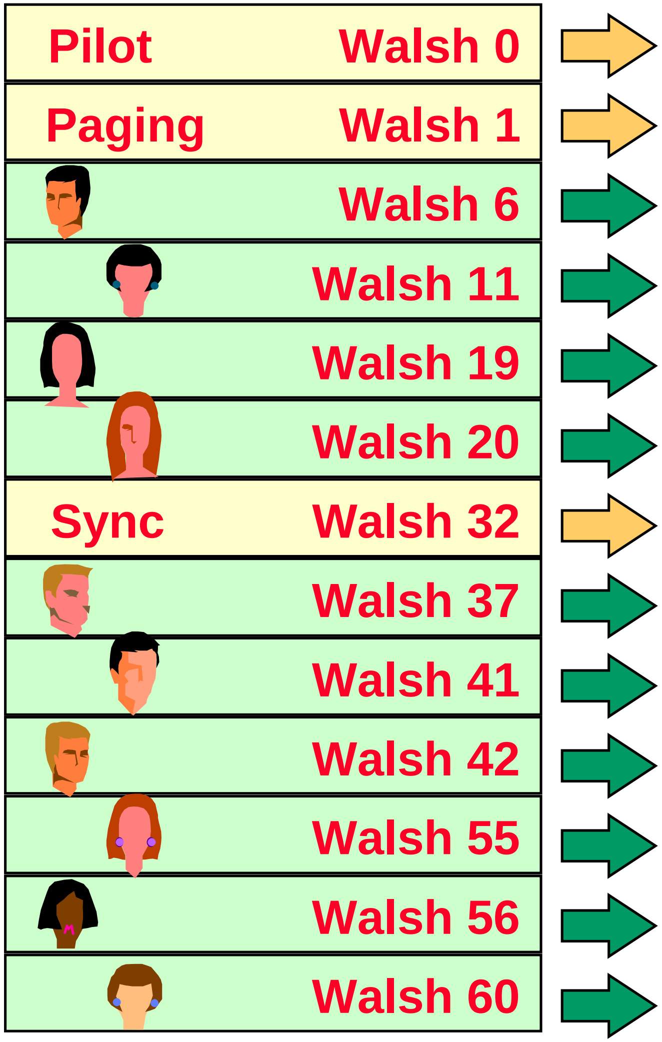
How a BTS Builds the Forward Code Channels



A Forward Channel is identified by:

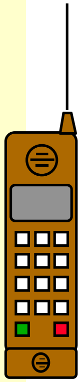
- its CDMA RF carrier Frequency
- the unique Short Code PN Offset of the sector
- the unique Walsh Code of the user

Functions of the CDMA Forward Channels

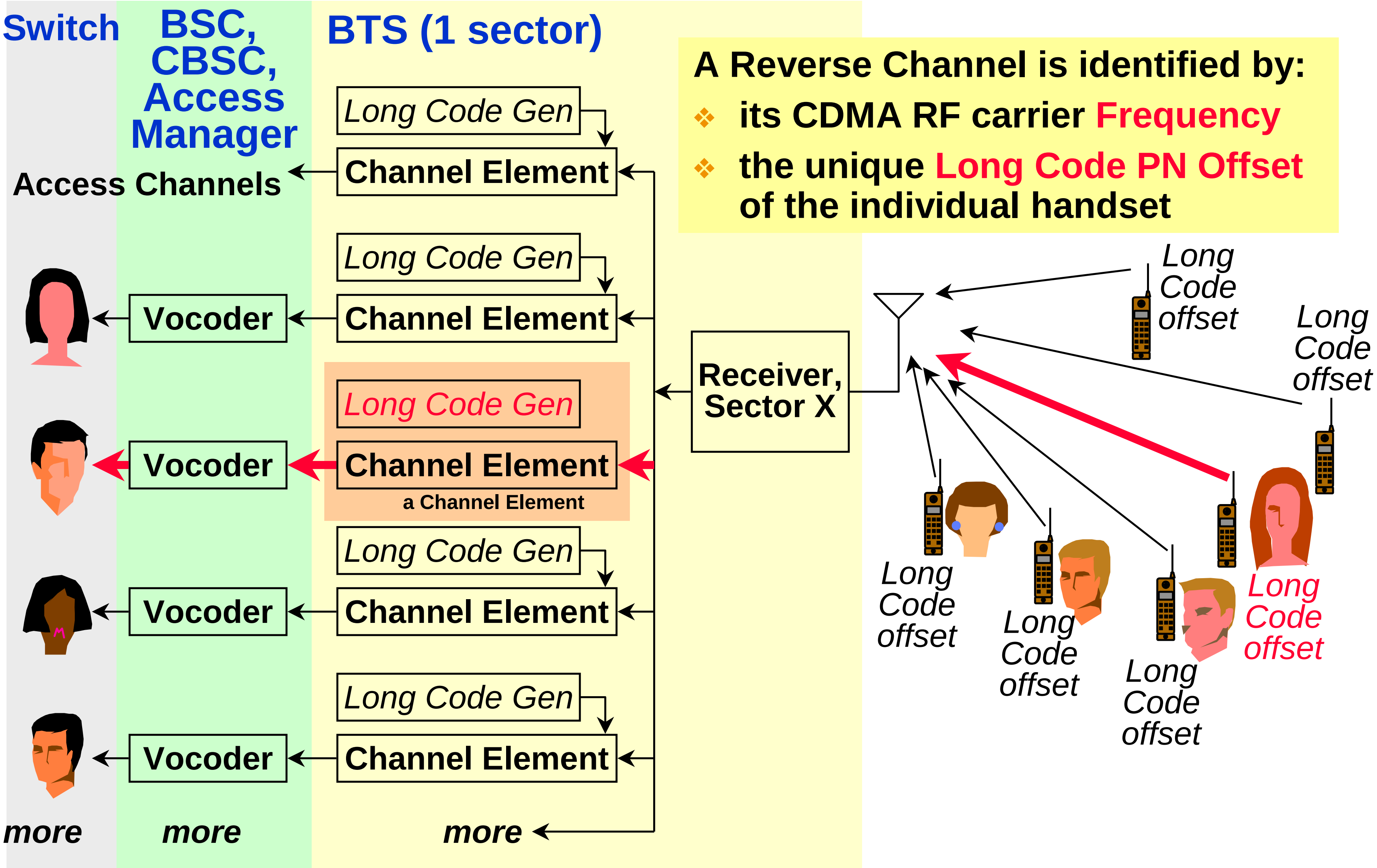


Pilot	Walsh 0
Paging	Walsh 1
	Walsh 6
	Walsh 11
	Walsh 19
	Walsh 20
Sync	Walsh 32
	Walsh 37
	Walsh 41
	Walsh 42
	Walsh 55
	Walsh 56
	Walsh 60

- **PILOT**: WALSH CODE **0**
  - The Pilot is a "structural beacon" which does not contain a character stream. It is a timing source used in system acquisition and as a measurement device during handoffs
- **SYNC**: WALSH CODE **32**
  - This carries a data stream of system identification and parameter information used by mobiles during system acquisition
- **PAGING**: WALSH CODES **1 up to 7**
  - There can be from one to seven paging channels as determined by capacity needs. They carry pages, system parameters information, and call setup orders
- **TRAFFIC**: any **remaining** WALSH codes
  - The traffic channels are assigned to individual users to carry call traffic. All remaining Walsh codes are available, subject to overall capacity limited by noise



Code Channels in the Reverse Direction

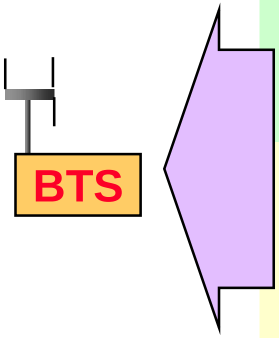


A Reverse Channel is identified by:

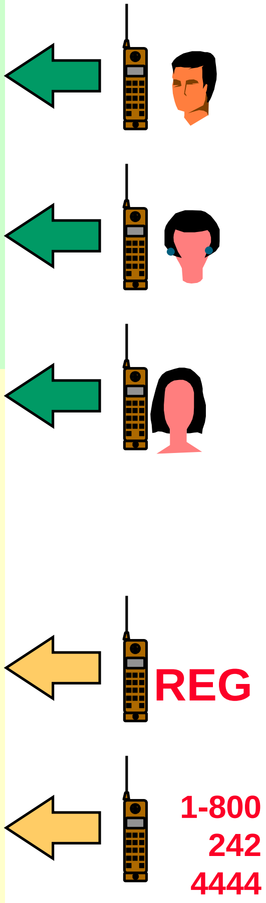
- **its CDMA RF carrier Frequency**
- **the unique Long Code PN Offset of the individual handset**

Functions of the CDMA Reverse Channels

There are two types of CDMA Reverse Channels:

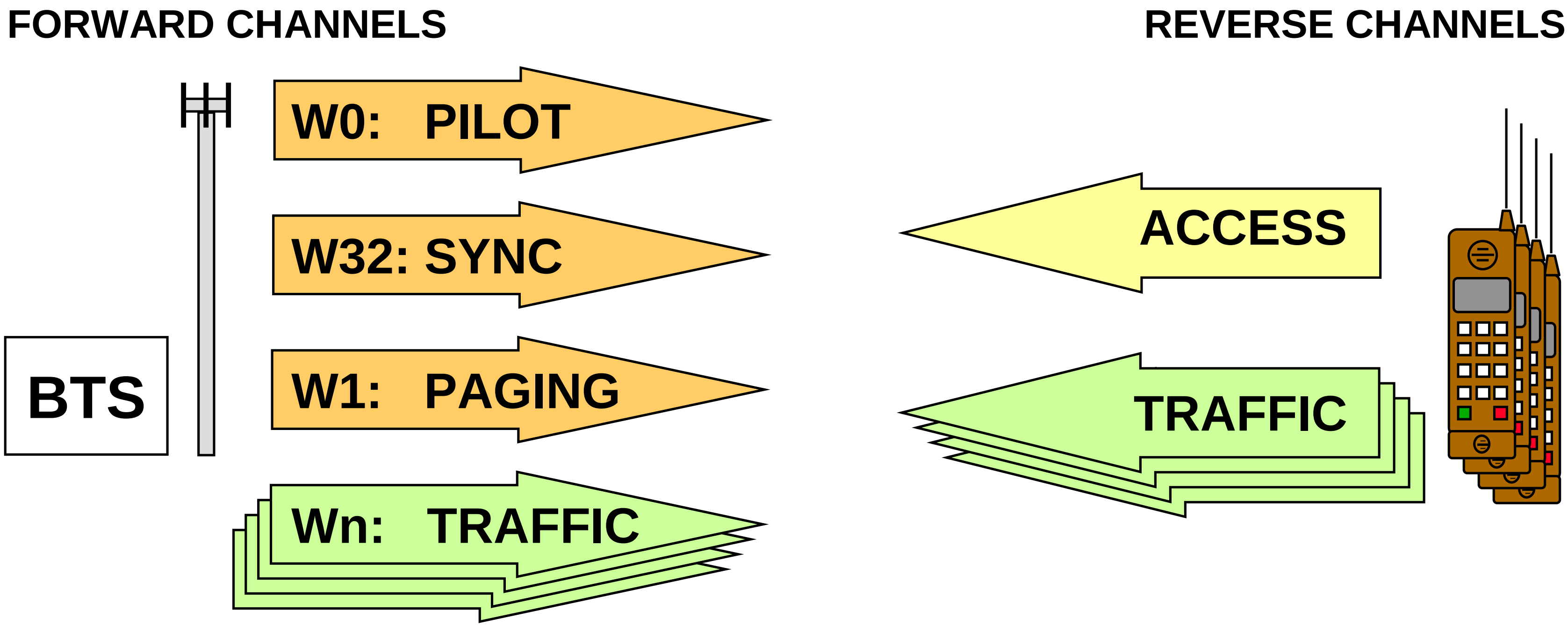


- **TRAFFIC CHANNELS** are used by individual users during their actual calls to transmit traffic to the BTS
  - a reverse traffic channel is really just a user-specific public or private Long Code mask
  - there are as many reverse Traffic Channels as there are CDMA phones in the world!
- **ACCESS CHANNELS** are used by mobiles not yet in a call to transmit registration requests, call setup requests, page responses, order responses, and other signaling information
  - an access channel is really just a public long code offset unique to the BTS sector
  - Access channels are paired to Paging Channels. Each paging channel can have up to 32 access channels.



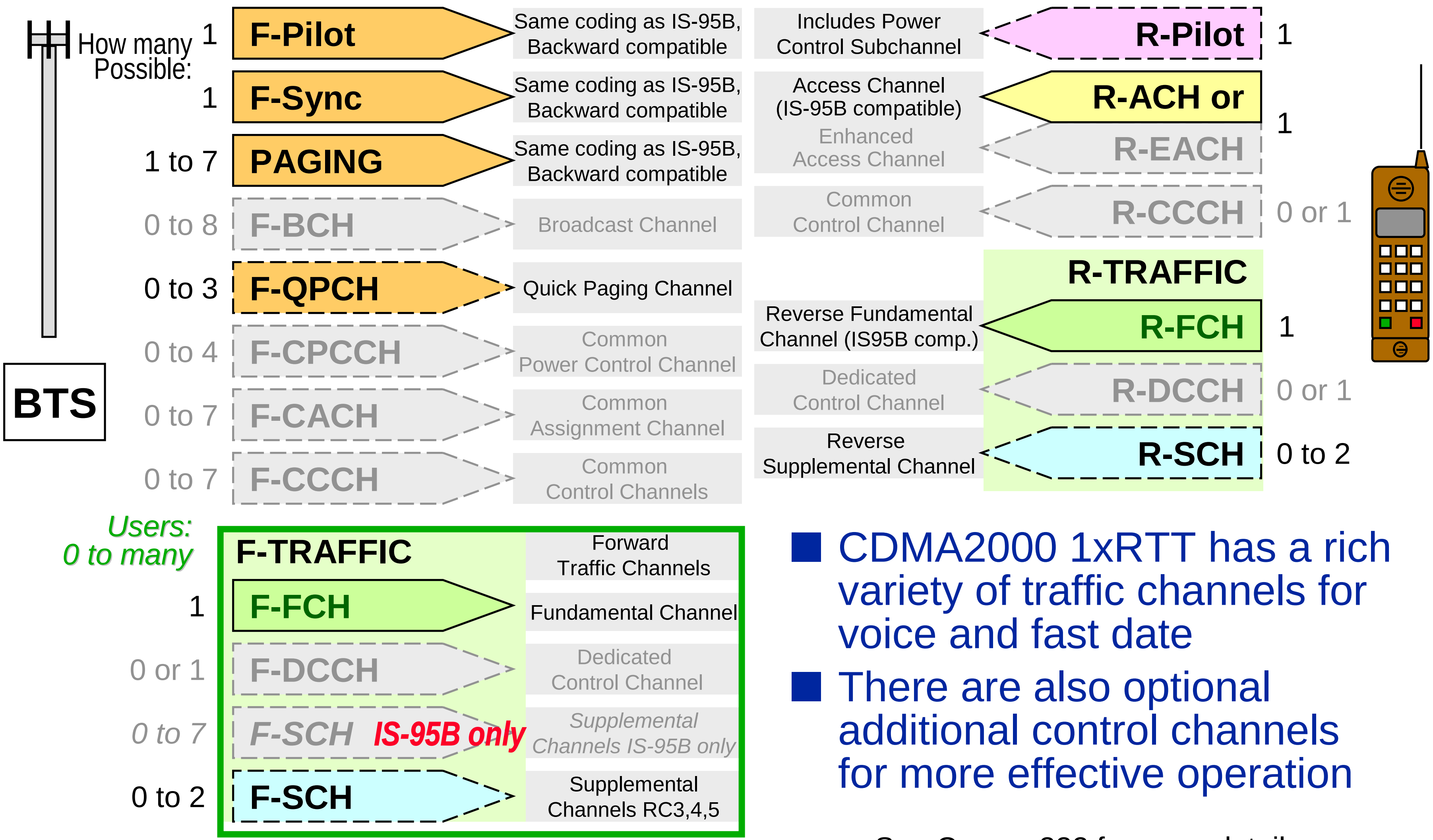
Although a sector can have up to seven paging channels, and each paging channel can have up to 32 access channels, nearly all systems today use only one paging channel per sector and only one access channel per paging channel.

Summing Up Original IS-95 CDMA Channels



- Existing IS-95A/JStd-008 CDMA uses the channels above for call setup and traffic channels – all call processing transactions use these channels
  - traffic channels are 9600 bps (rate set 1) or 14400 bps (rate set 2)
- IS-2000 CDMA is backward-compatible with IS-95, but offers additional radio configurations and additional kinds of possible channels
  - These additional modes are called Radio Configurations
  - IS-95 Rate Set 1 and 2 are IS-2000 Radio Configurations 1 & 2

The Channels at Phase One 1xRTT Launch



FORWARD CHANNELS

REVERSE CHANNELS

BTS

How many Possible:

1	**F-Pilot**	Same coding as IS-95B, Backward compatible
1	**F-Sync**	Same coding as IS-95B, Backward compatible
1 to 7	**PAGING**	Same coding as IS-95B, Backward compatible
0 to 8	**F-BCH**	Broadcast Channel
0 to 3	**F-QPCH**	Quick Paging Channel
0 to 4	**F-CPCCH**	Common Power Control Channel
0 to 7	**F-CACH**	Common Assignment Channel
0 to 7	**F-CCCH**	Common Control Channels

Users: 0 to many

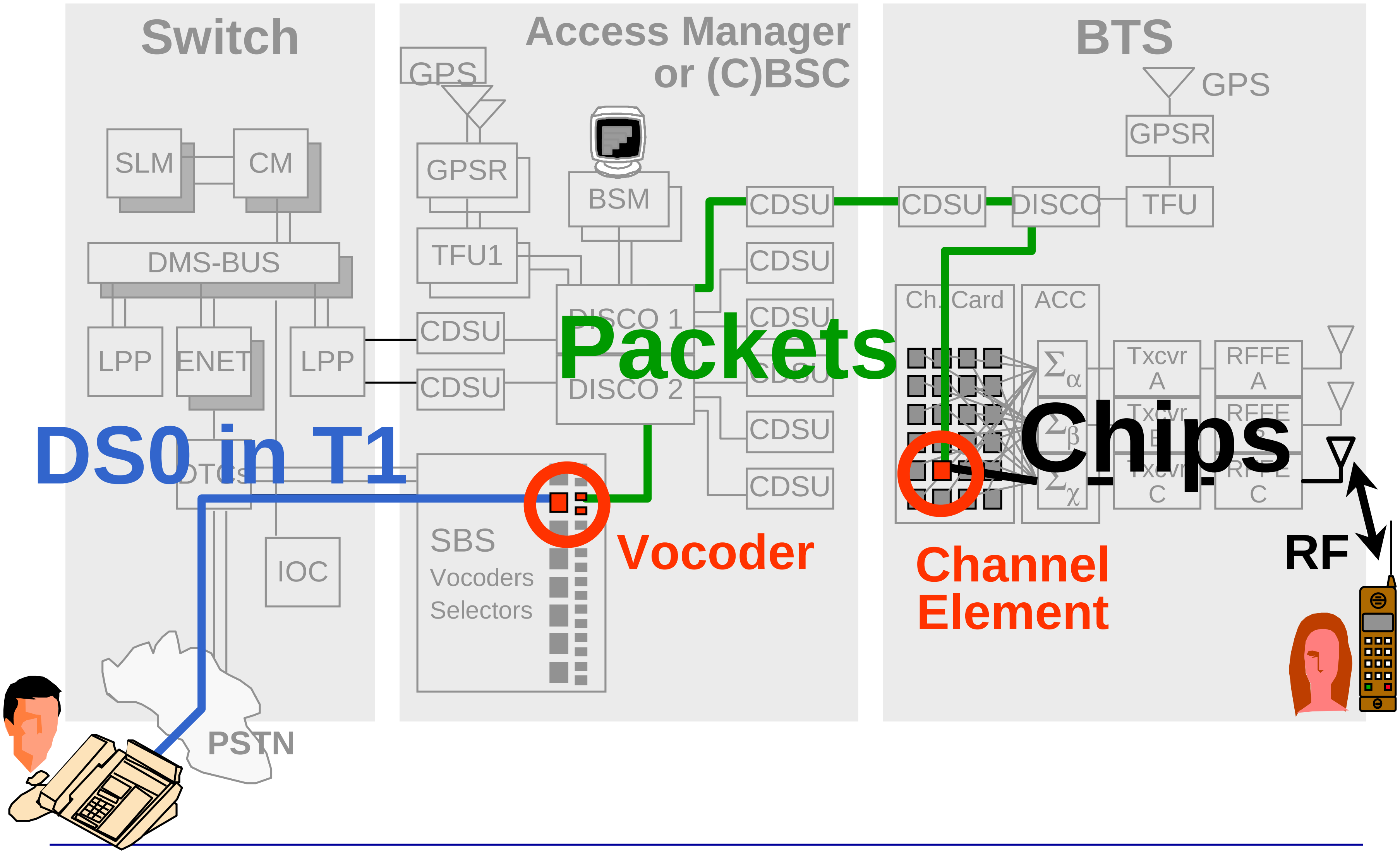
	F-TRAFFIC	Forward Traffic Channels
1	**F-FCH**	Fundamental Channel
0 or 1	**F-DCCH**	Dedicated Control Channel
0 to 7	***F-SCH*** ***IS-95B only***	*Supplemental Channels IS-95B only*
0 to 2	**F-SCH**	Supplemental Channels RC3,4,5

Includes Power Control Subchannel	**R-Pilot**	1
Access Channel (IS-95B compatible)	**R-ACH or**	1
Enhanced Access Channel	**R-EACH**	
Common Control Channel	**R-CCCH**	0 or 1
	R-TRAFFIC	
Reverse Fundamental Channel (IS95B comp.)	**R-FCH**	1
Dedicated Control Channel	**R-DCCH**	0 or 1
Reverse Supplemental Channel	**R-SCH**	0 to 2

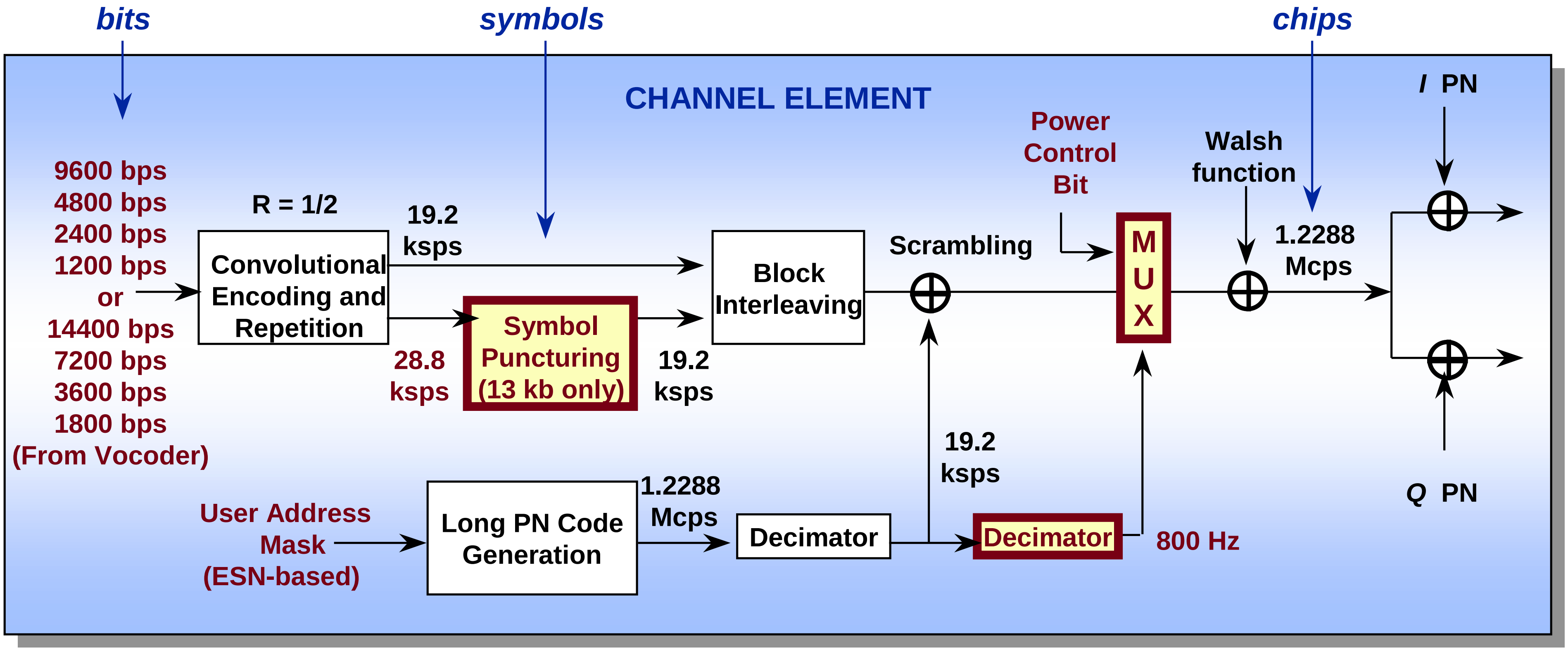
- CDMA2000 1xRTT has a rich variety of traffic channels for voice and fast date
- There are also optional additional control channels for more effective operation

See Course 332 for more details.

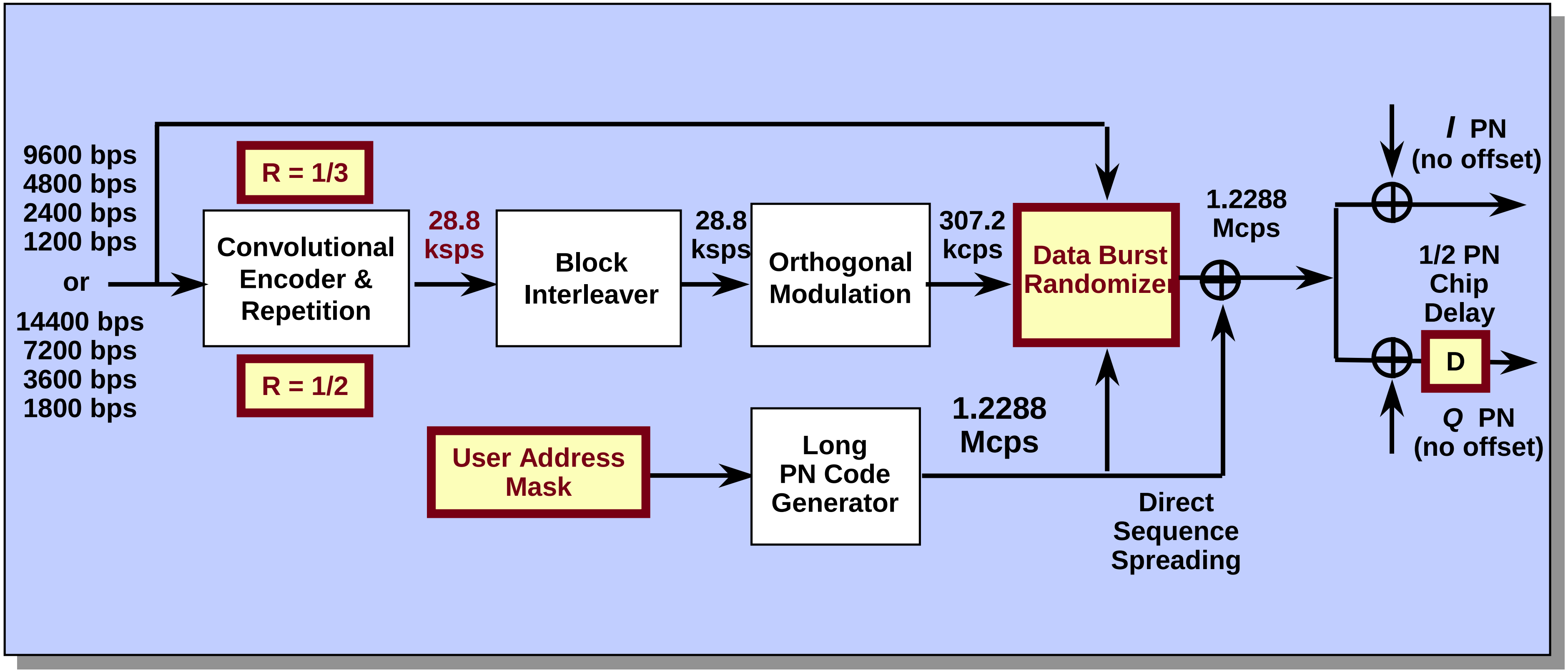
Basic CDMA Network Architecture



Forward Traffic Channel: Generation Details from IS-95



Reverse Traffic Channel: Generation Details from IS-95



Section C

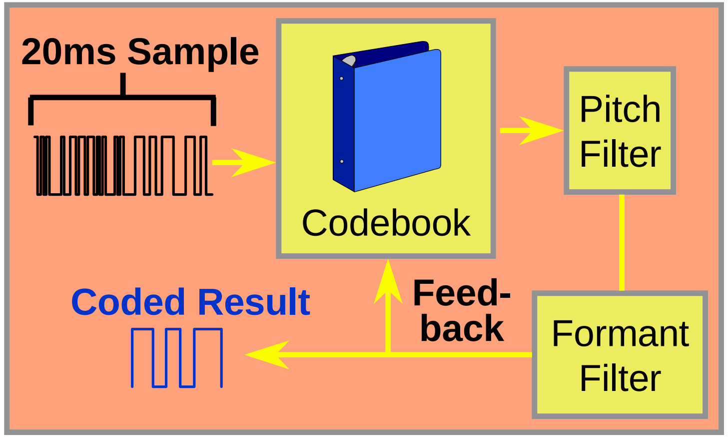
IS-95 Operational Details

Vocoding, Multiplexing, Power Control

Variable Rate Vocoding & Multiplexing

- Vocoders compress speech, reduce bit rate, greatly increasing capacity
- CDMA uses a superior Variable Rate Vocoder
  - full rate during speech
  - low rates in speech pauses
  - increased capacity
  - more natural sound
- Voice, signaling, and user secondary data may be mixed in CDMA frames

DSP QCELP VOCODER



bits	Frame Sizes
192/288	Full Rate Frame
96/144	1/2 Rate Frame
48/72	1/4 Rt.
24/36	1/8

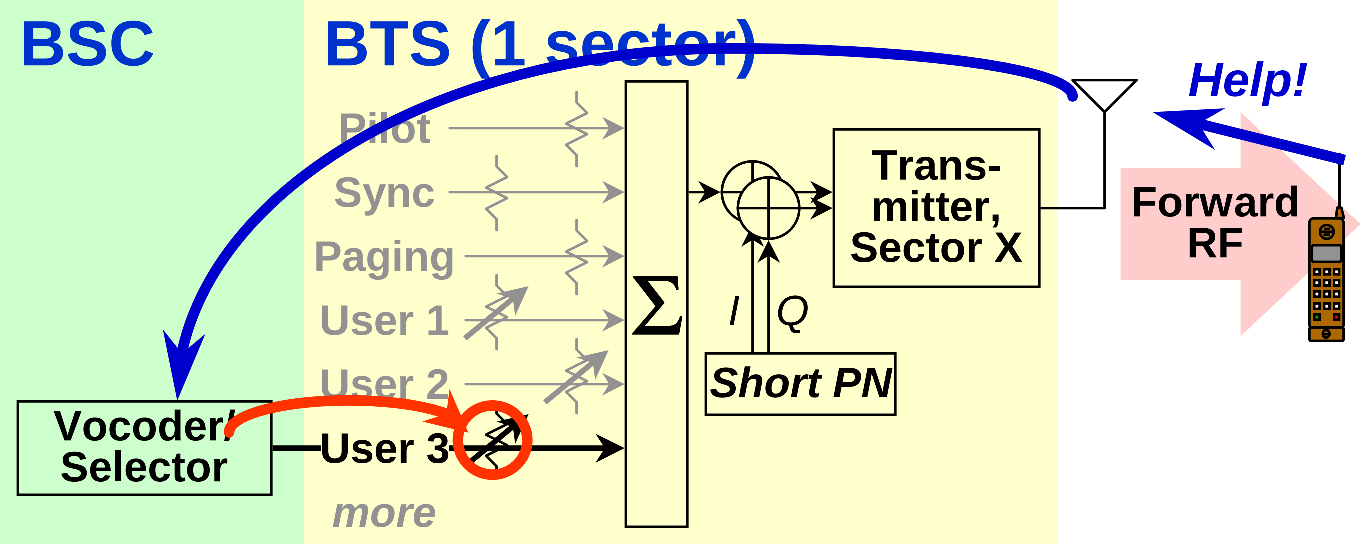
Frame Contents: can be a mixture of

Primary Traffic (Voice or data)

Signaling (System Messaging)

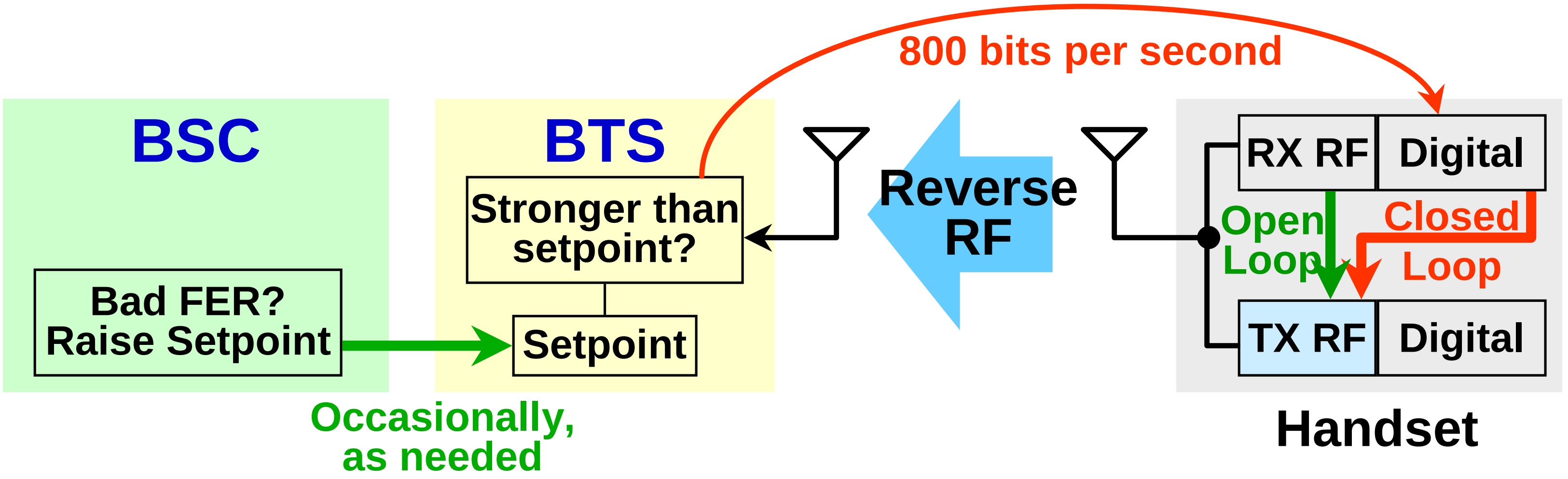
Secondary (On-Air activation, etc)

Forward Power Control



- The BTS continually reduces the strength of each user’s forward baseband chip stream
- When a particular handset sees errors on the forward link, it requests more energy
- The complainer’s chip stream gets a quick boost; afterward, continues to diminish
- Each network manufacturer uses FER-based triggers and initial, minimum, and maximum traffic channel DGU values
- *In CDMA2000, there is a faster method used for Forward Power Control operating much like the IS-95 Reverse Link Power control described next*

Reverse Power Control



- Three methods work in tandem to equalize all handset signal levels at the BTS
  - Reverse *Open* Loop: handset adjusts power up or down based on received BTS signal (AGC)
  - Reverse *Closed* Loop: Is handset too strong? BTS tells up or down 1 dB 800 times/second
  - Reverse *Outer* Loop: BSC has FER trouble hearing handset? BSC adjusts BTS setpoint

Details of Reverse Link Power Control

TXPO Handset Transmit Power

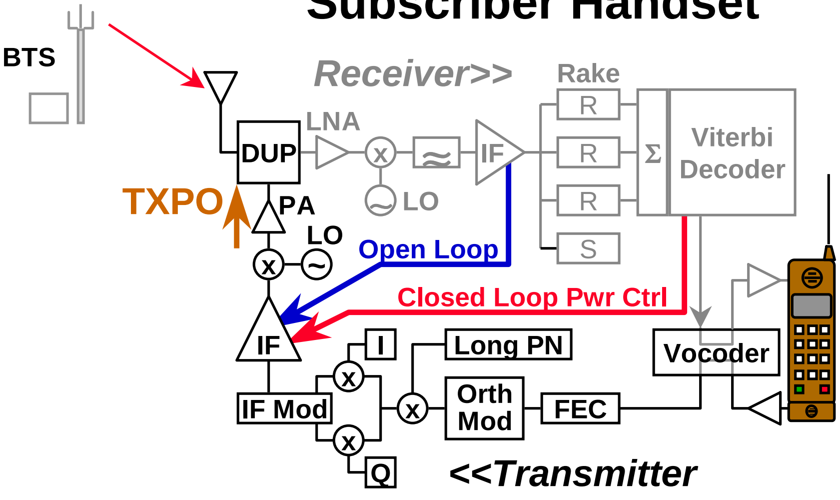
- Actual RF power output of the handset transmitter, including combined effects of **open loop power control** from receiver AGC *and* **closed loop power control** by BTS
- can't exceed handset's maximum (typ. +23 dBm)

$TXPO = -(RX_{dbm}) - C + TXGA$
C = +73 for 800 MHz. systems
= +76 for 1900 MHz. systems

TXGA Transmit Gain Adjust

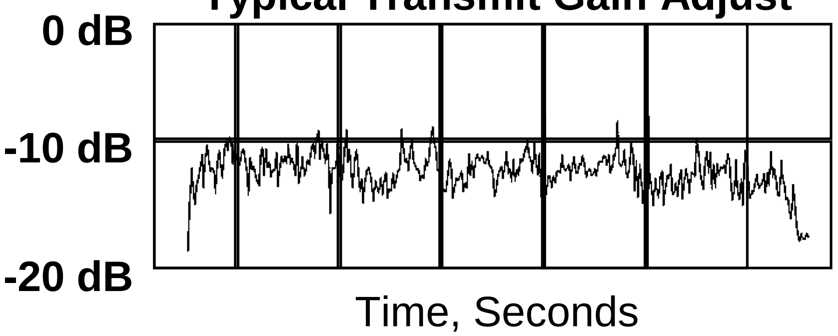
- Sum of all **closed-loop power control** commands from the BTS since the beginning of this call

Subscriber Handset



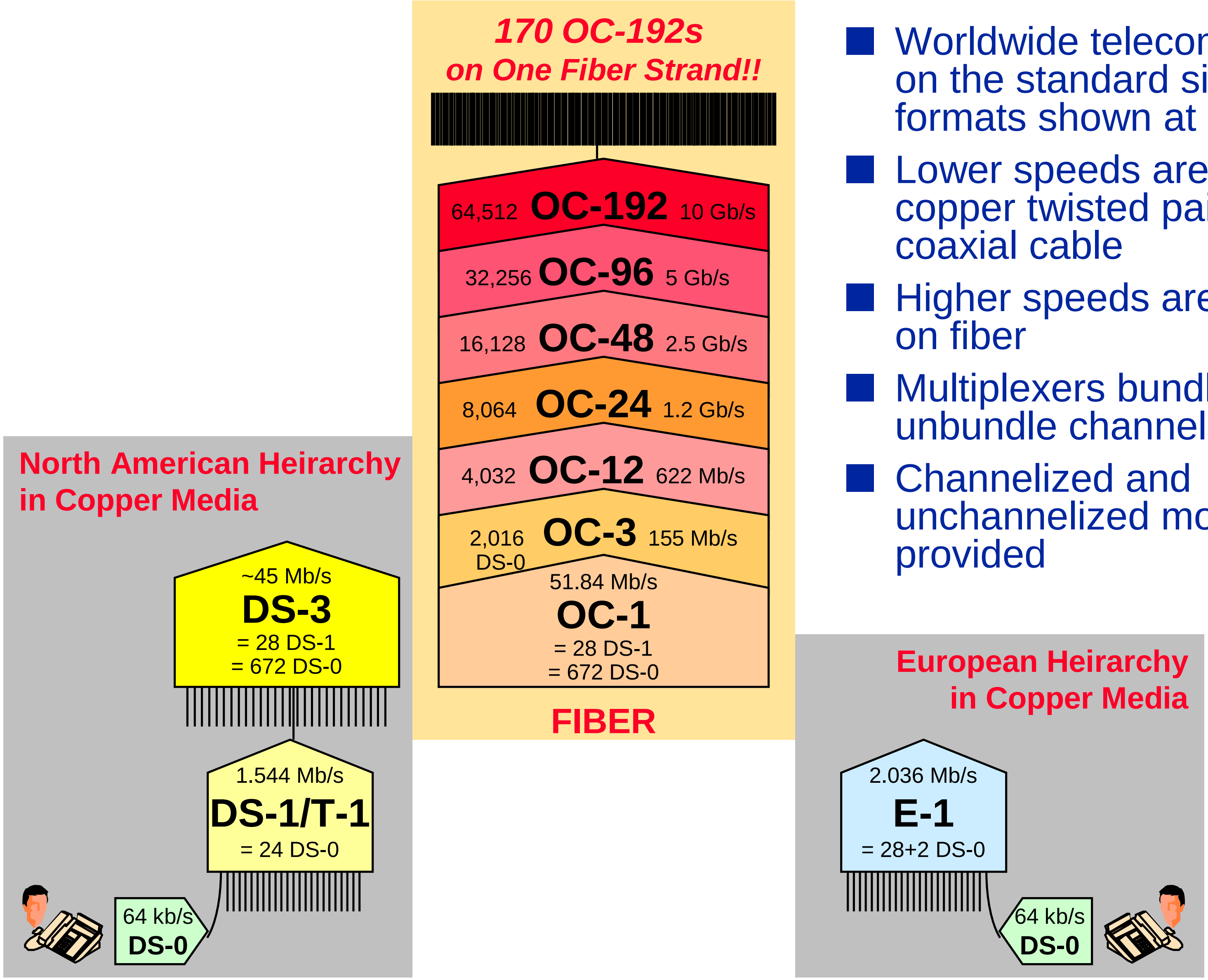
Typical TXPO:
+23 dBm in a coverage hole
0 dBm near middle of cell
-50 dBm up close to BTS

Typical Transmit Gain Adjust



CDMA Network Architecture

Telecom Transmission Standards



170 OC-192s on One Fiber Strand!!

64,512 **OC-192** 10 Gb/s

32,256 **OC-96** 5 Gb/s

16,128 **OC-48** 2.5 Gb/s

8,064 **OC-24** 1.2 Gb/s

4,032 **OC-12** 622 Mb/s

2,016 DS-0 **OC-3** 155 Mb/s

51.84 Mb/s **OC-1** = 28 DS-1 = 672 DS-0

FIBER

North American Heirarchy in Copper Media

~45 Mb/s **DS-3** = 28 DS-1 = 672 DS-0

1.544 Mb/s **DS-1/T-1** = 24 DS-0

64 kb/s **DS-0**

European Heirarchy in Copper Media

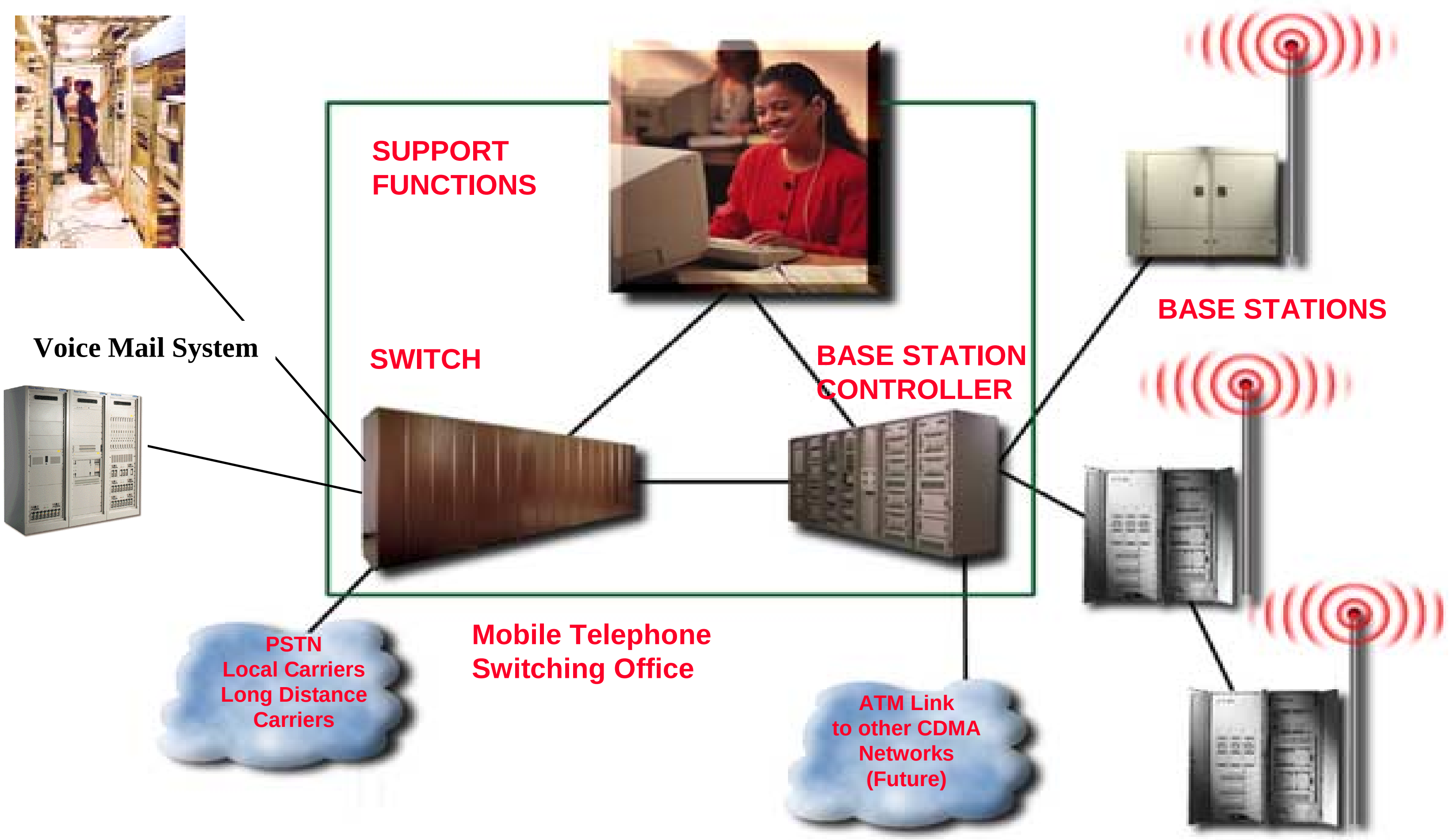
2.036 Mb/s **E-1** = 28+2 DS-0

64 kb/s **DS-0**

- Worldwide telecom rides on the standard signal formats shown at left
- Lower speeds are used on copper twisted pairs or coaxial cable
- Higher speeds are carried on fiber
- Multiplexers bundle and unbundle channels
- Channelized and unchannelized modes are provided

Structure of a Typical CDMA System

HLR Home Location Register
(subscriber database)



Voice Mail System

SUPPORT
FUNCTIONS

SWITCH

BASE STATION
CONTROLLER

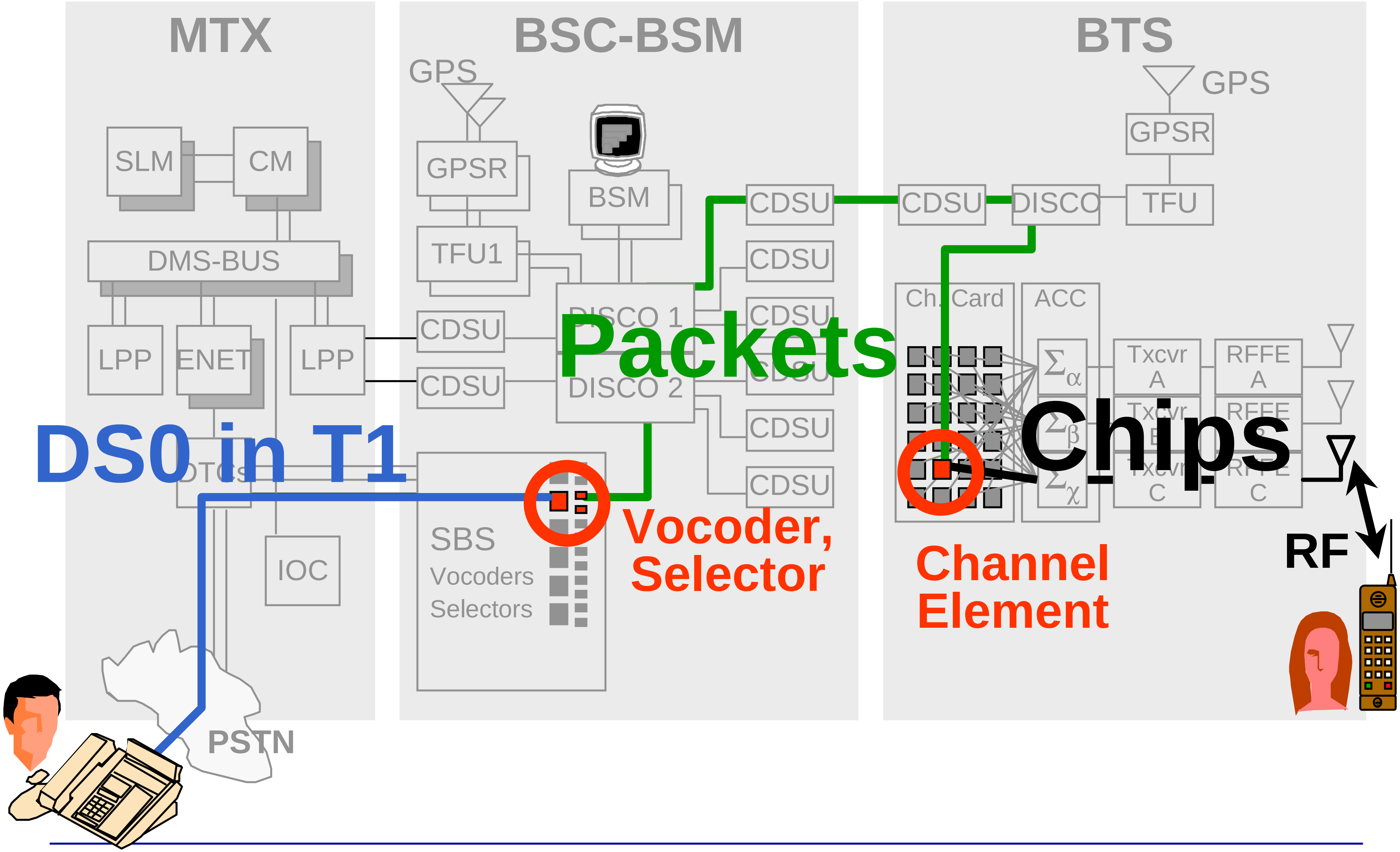
BASE STATIONS

PSTN
Local Carriers
Long Distance
Carriers

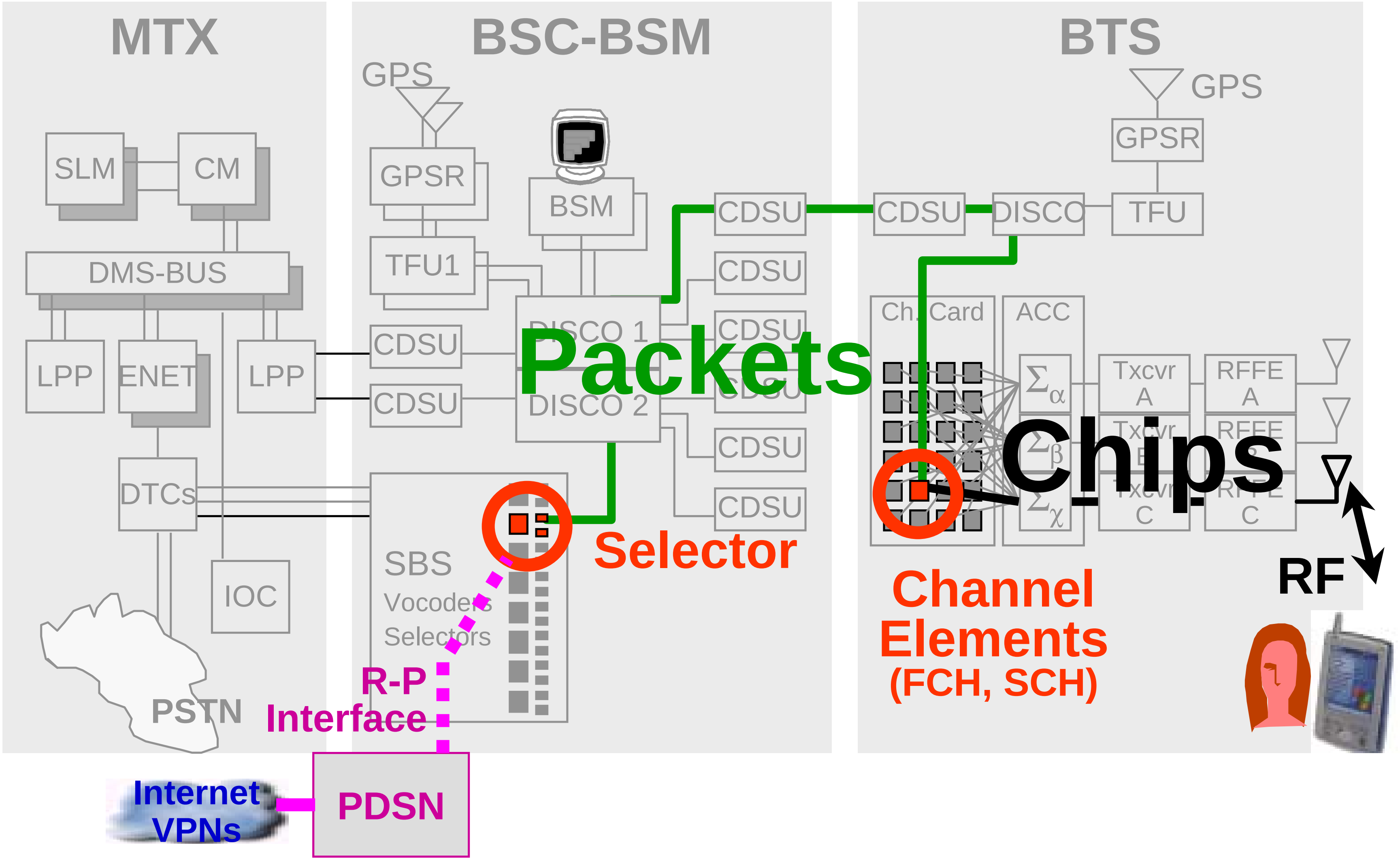
Mobile Telephone
Switching Office

ATM Link
to other CDMA
Networks
(Future)

Voice Call Path through the CDMA Network



1x Data Call Path through the CDMA Network



Section D

A Quick Introduction to CDMA Messages and Call Processing

Messages in CDMA

- In CDMA, most call processing events are driven by messages
- Some CDMA channels exist for the sole purpose of carrying messages; they never carry user’s voice traffic
    - Sync Channel (a forward channel)
    - Paging Channel (a forward channel)
    - Access Channel (a reverse channel)
    - On these channels, there are only messages, continuously all of the time
- Some CDMA channels exist just to carry user traffic
    - Forward Traffic Channel
    - Reverse Traffic Channel
    - On these channels, most of the time is filled with traffic and messages are sent only when there is something to do
- All CDMA messages have very similar structure, regardless of the channel on which they are sent

How CDMA Messages are Sent

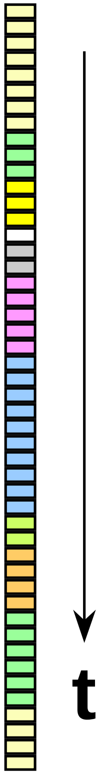
- CDMA messages on both forward and reverse traffic channels are normally sent via dim-and-burst
- Messages include many fields of binary data
- The first byte of each message identifies message type: this allows the recipient to parse the contents
- To ensure no messages are missed, all CDMA messages bear serial numbers and important messages contain a bit requesting acknowledgment
- Messages not promptly acknowledged are retransmitted several times. If not acknowledged, the sender may release the call
- Field data processing tools capture and display the messages for study

EXAMPLE:
A POWER MEASUREMENT REPORT MESSAGE

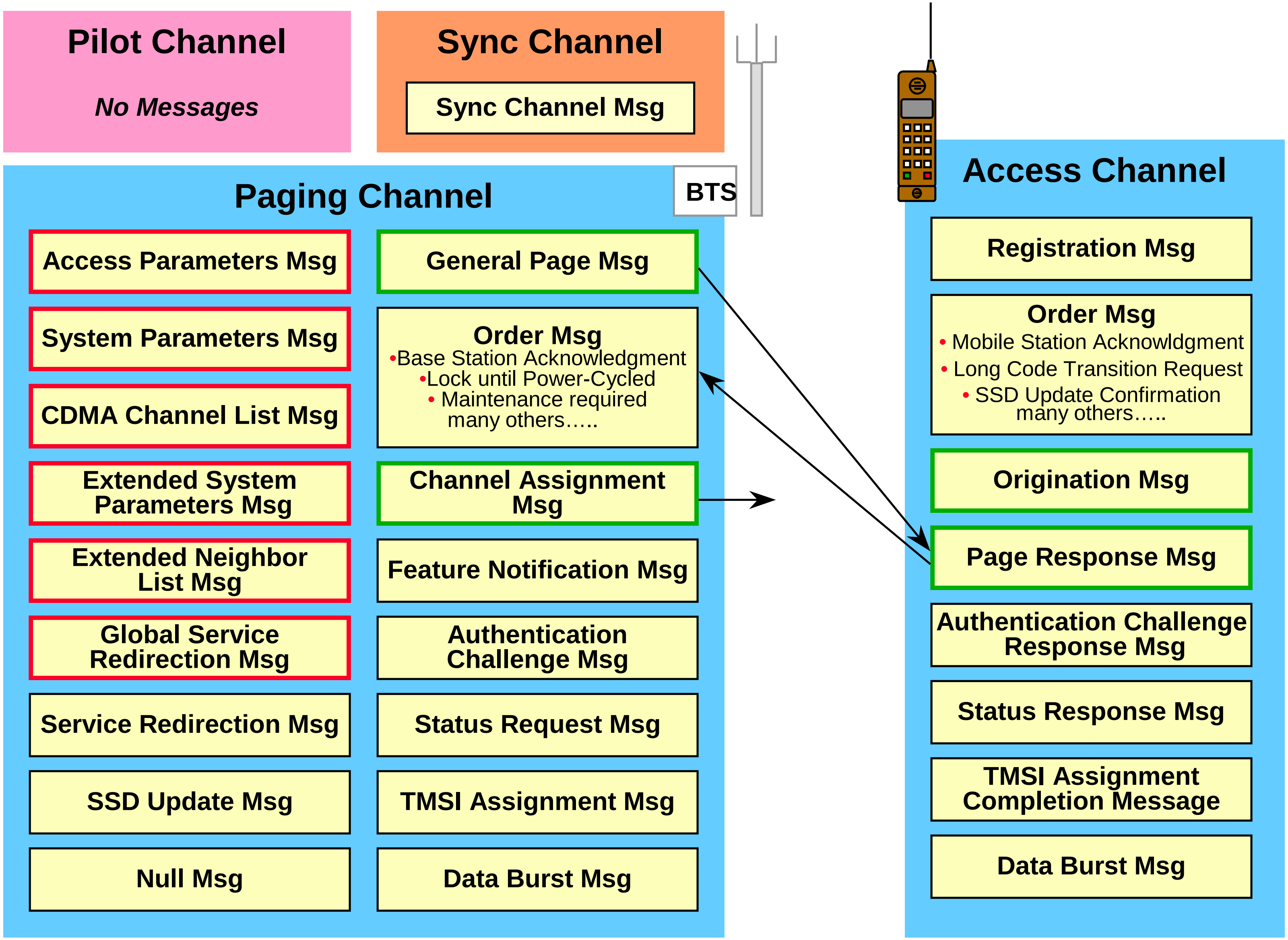
Field	Length (in bits)
MSG_TYPE (‘00000110’)	8
ACK_SEQ	3
MSG_SEQ	3
ACK_REQ	1
ENCRYPTION	2
ERRORS_DETECTED	5
POWER_MEAS_FRAMES	10
LAST_HDM_SEQ	2
NUM_PILOTS	4

NUM_PILOTS occurrences of this field:

PILOT_STRENGTH	6
RESERVED (‘0’s)	0-7



Message Vocabulary: Acquisition & Idle States



Pilot Channel

No Messages

Sync Channel

- **Sync Channel Msg**

Paging Channel

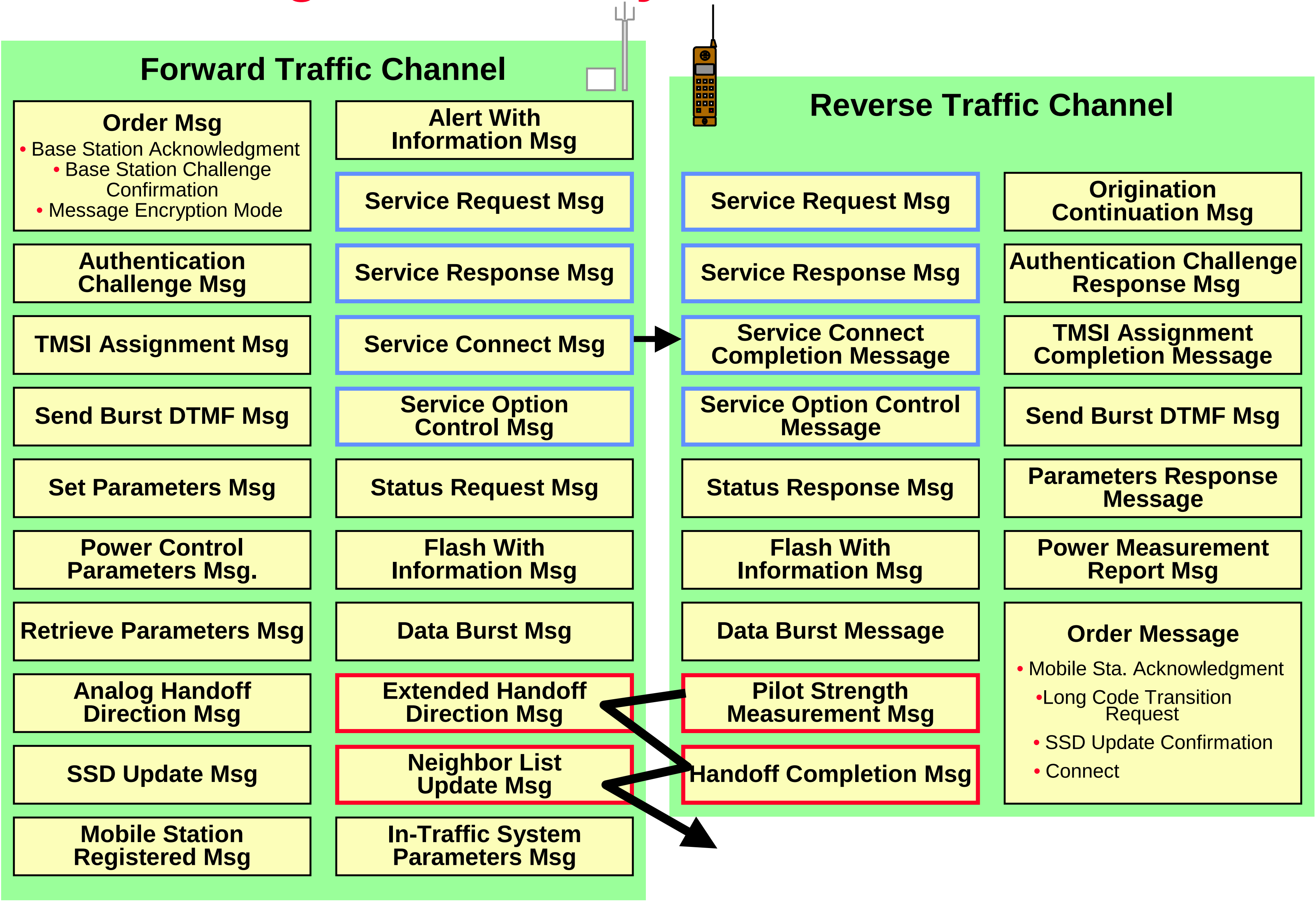
BTS

- **Access Parameters Msg**
- **System Parameters Msg**
- **CDMA Channel List Msg**
- **Extended System Parameters Msg**
- **Extended Neighbor List Msg**
- **Global Service Redirection Msg**
- **Service Redirection Msg**
- **SSD Update Msg**
- **Null Msg**
- **General Page Msg**
- **Order Msg**
  - Base Station Acknowledgment
  - Lock until Power-Cycled
  - Maintenance required
  - many others…..
- **Channel Assignment Msg**
- **Feature Notification Msg**
- **Authentication Challenge Msg**
- **Status Request Msg**
- **TMSI Assignment Msg**
- **Data Burst Msg**

Access Channel

- **Registration Msg**
- **Order Msg**
  - Mobile Station Acknowldgment
  - Long Code Transition Request
  - SSD Update Confirmation
  - many others…..
- **Origination Msg**
- **Page Response Msg**
- **Authentication Challenge Response Msg**
- **Status Response Msg**
- **TMSI Assignment Completion Message**
- **Data Burst Msg**

Message Vocabulary: Conversation State



Forward Traffic Channel

Order Msg
- Base Station Acknowledgment
- Base Station Challenge Confirmation
- Message Encryption Mode

Authentication Challenge Msg

TMSI Assignment Msg

Send Burst DTMF Msg

Set Parameters Msg

Power Control Parameters Msg.

Retrieve Parameters Msg

Analog Handoff Direction Msg

SSD Update Msg

Mobile Station Registered Msg

Alert With Information Msg

Service Request Msg

Service Response Msg

Service Connect Msg

Service Option Control Msg

Status Request Msg

Flash With Information Msg

Data Burst Msg

Extended Handoff Direction Msg

Neighbor List Update Msg

In-Traffic System Parameters Msg

Reverse Traffic Channel

Service Request Msg

Service Response Msg

Service Connect Completion Message

Service Option Control Message

Status Response Msg

Flash With Information Msg

Data Burst Message

Pilot Strength Measurement Msg

Handoff Completion Msg

Origination Continuation Msg

Authentication Challenge Response Msg

TMSI Assignment Completion Message

Send Burst DTMF Msg

Parameters Response Message

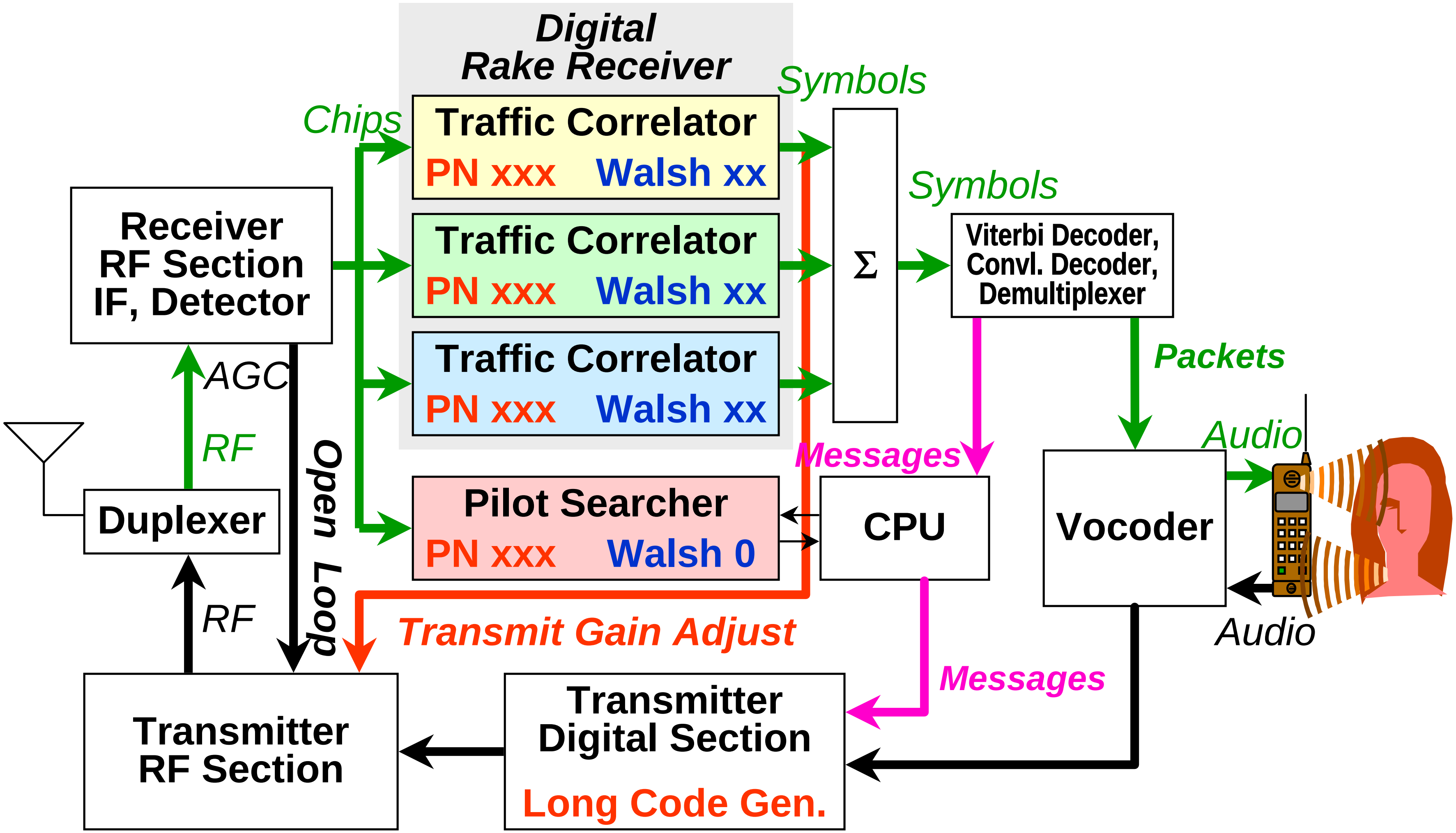
Power Measurement Report Msg

Order Message
- Mobile Sta. Acknowledgment
- Long Code Transition Request
- SSD Update Confirmation
- Connect

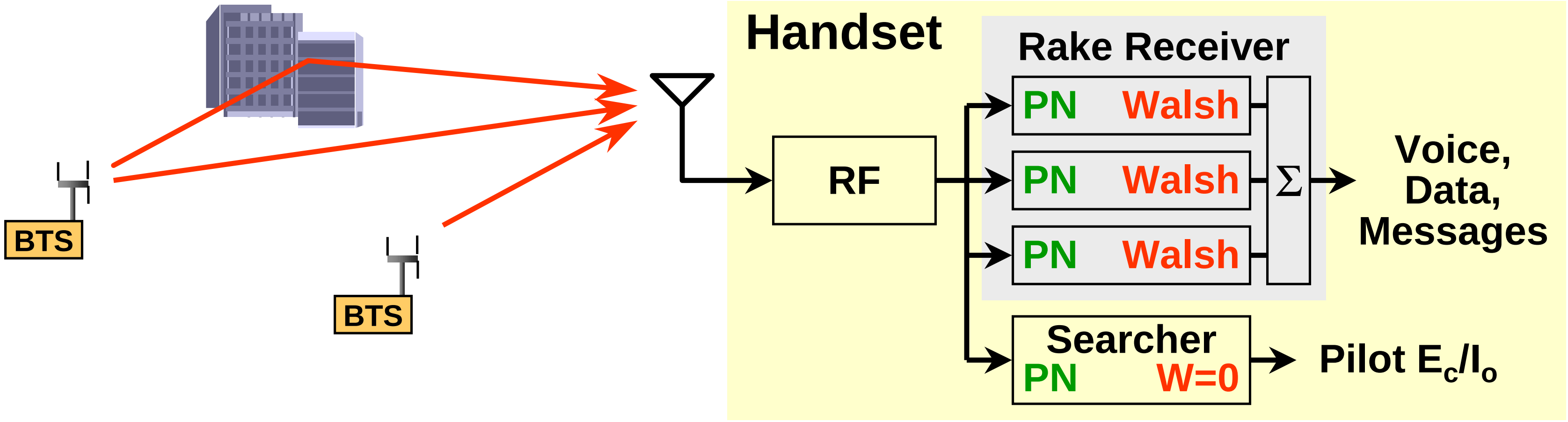
Section E

CDMA Handset Architecture
CDMA Handoffs

What’s In a Handset? How does it work?

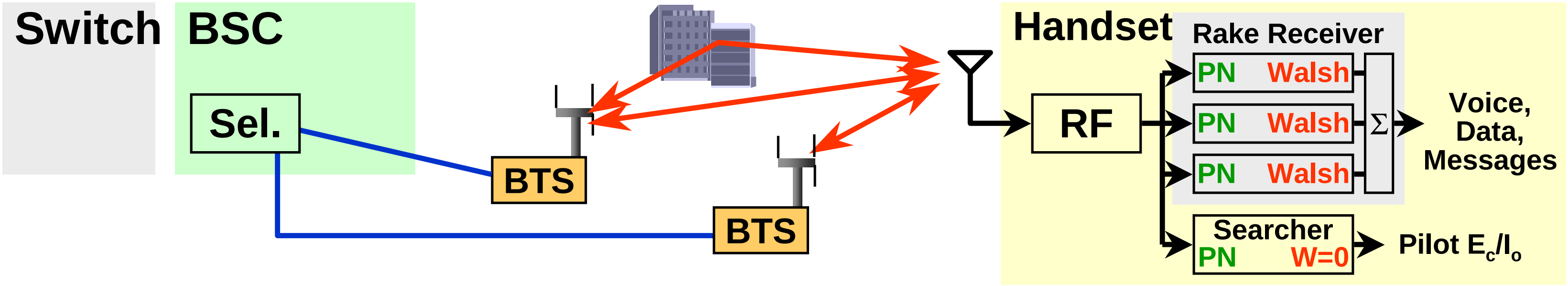


The Rake Receiver



- Every frame, handset uses combined outputs of the three traffic correlators (“rake fingers”)
- Each finger can independently recover a particular PN offset and Walsh code
- Fingers can be targeted on delayed multipath reflections, or even on different BTSs
- Searcher continuously checks pilots

CDMA Soft Handoff Mechanics

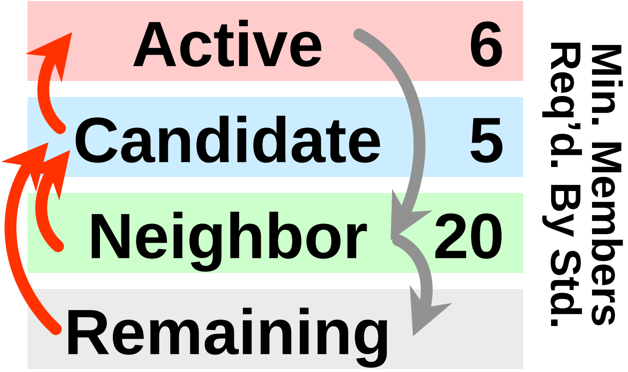


- CDMA soft handoff is driven by the handset
  - Handset continuously checks available pilots
  - Handset tells system pilots it currently sees
  - System assigns sectors (up to 6 max.), tells handset
  - Handset assigns its fingers accordingly
  - All messages sent by dim-and-burst, no muting!
- Each end of the link chooses what works best, on a frame-by-frame basis!
  - Users are totally unaware of handoff

The Complete Rules of Soft Handoff

- The Handset considers pilots in ***sets***
  - **Active**: pilots of sectors actually in use
  - **Candidates**: pilots mobile requested, but not yet set up & transmitting by system
  - **Neighbors**: pilots told to mobile by system, as nearby sectors to check
  - **Remaining**: any pilots used by system but not already in the other sets (div. by PILOT_INC)
- Handset sends **Pilot Strength Measurement Message** to the system whenever:
  - It notices a pilot in neighbor or remaining set exceeds **T_ADD**
  - An active set pilot drops below **T_DROP** for **T_TDROP** time
  - A candidate pilot exceeds an active by **T_COMP**
- The System may set up all requested handoffs, or it may apply special manufacturer-specific screening criteria and only authorize some

PILOT SETS



Min. Members Req'd. By Std.

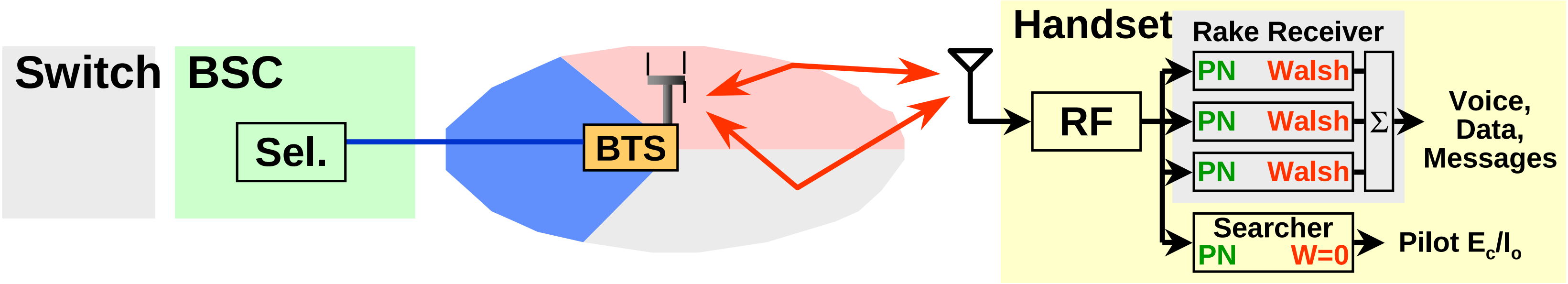
Active	6
Candidate	5
Neighbor	20
Remaining	

HANDOFF PARAMETERS

T_ADD	T_DROP
T_TDROP	T_COMP

Exercise: How does a pilot in one set migrate into another set, for all cases? Identify the trigger, and the messages involved.

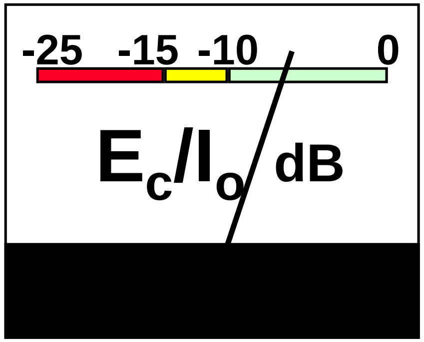
Softer Handoff



- Each BTS sector has unique PN offset & pilot
- Handset will ask for whatever pilots it wants
- If multiple sectors of one BTS simultaneously serve a handset, this is called Softer Handoff
- Handset can't tell the difference, but ***softer*** handoff occurs in BTS in a single channel element
- Handset can even use combination soft-softer handoff on multiple BTS & sectors

What is Ec/Io?

- E_c/I_o
  - “cleanness” of the pilot
    - foretells the readability of the associated traffic channels
  - guides soft handoff decisions
  - digitally derived: ratio of good to bad energy seen by the search correlator at the desired PN offset
  - Never appears higher than Pilot’s percentage of serving cell’s transmitted energy
  - Can be degraded by strong RF from other cells, sectors
    - Imperfect orthogonality, other PNs are ~-20 dB.
  - Can be degraded by noise



E_c **Energy of desired pilot alone**

I_o **Total energy received**

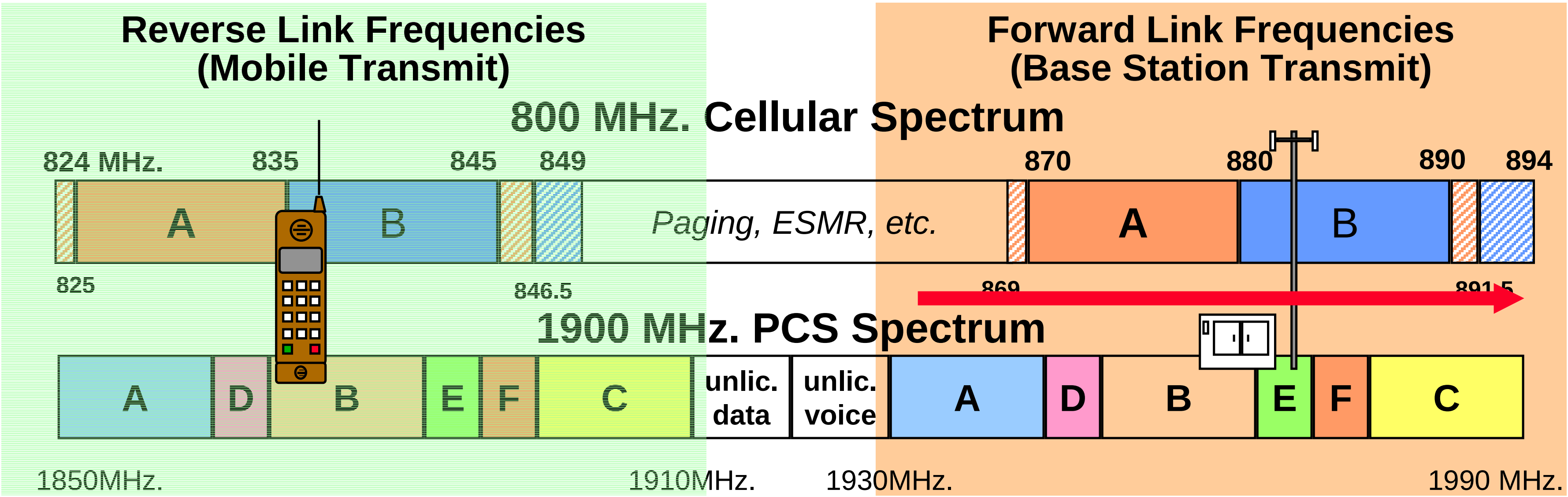
Section F

CDMA Call Processing

Example 1

Let’s Acquire the System!

Find a Frequency with a CDMA RF Signal



Mobile scans forward link frequencies:

(Cellular or PCS, depending on model)

History List

Preferred Roaming List

until a CDMA signal is found.

NO CDMA?! Go to AMPS,

or to a power-saving standby mode

FREQUENCY LISTS:

HISTORY LIST/MRU

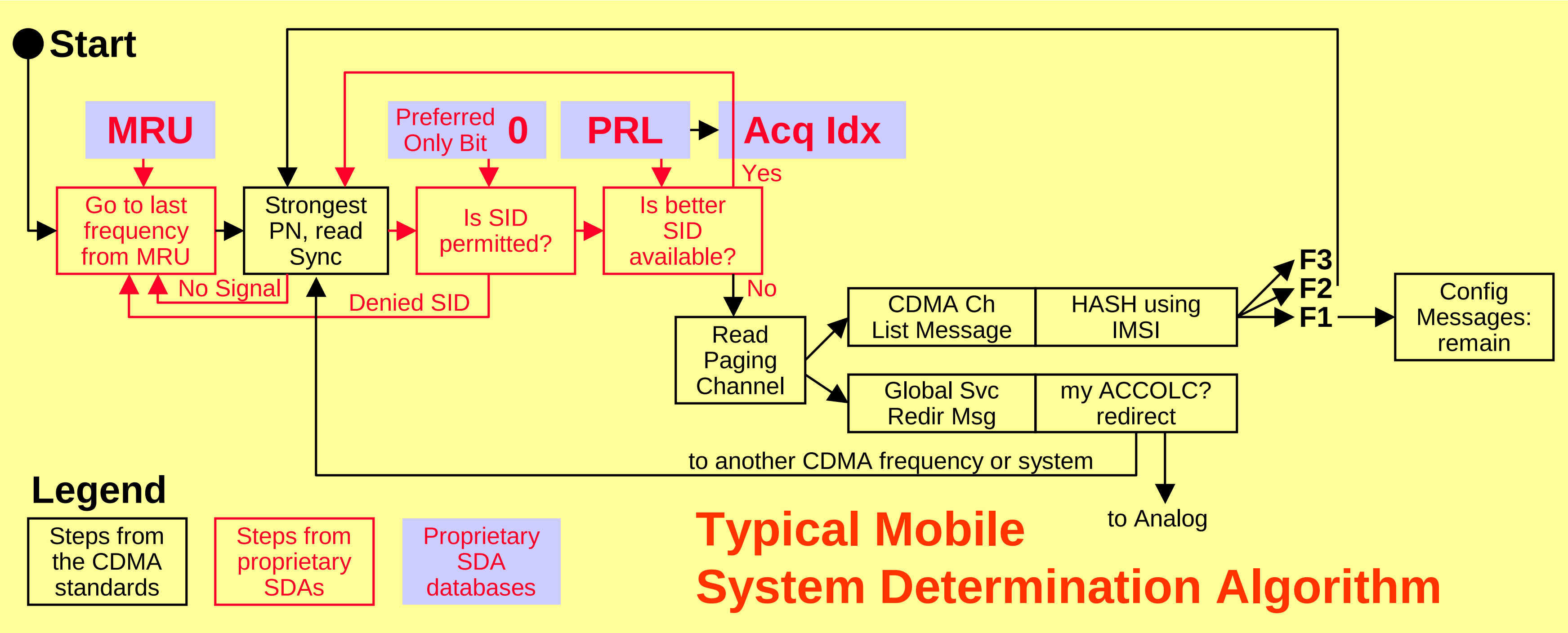
Last-used:
Freq
Freq
Freq
Freq
Freq
etc.

PREFERRED ROAMING LIST/PRL

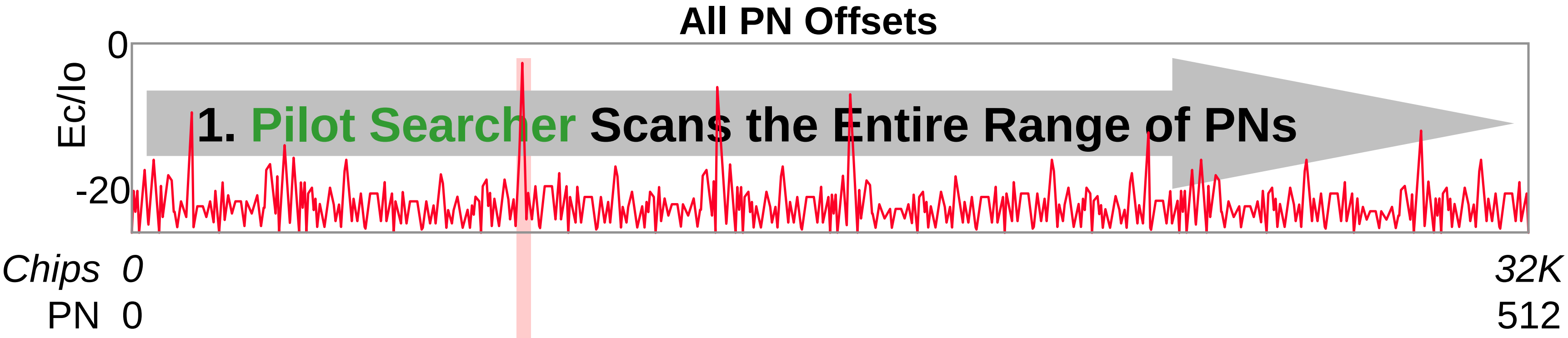
System1
System2
System3
System4
System5
etc.

How Idle Mobiles Choose CDMA Carriers

- At turnon, Idle mobiles use proprietary algorithms to find the initial CDMA carrier intended for them to use
- Within that CDMA signal, two types of paging channel messages could cause the idle mobile to choose another frequency: CDMA Channel List Message and GSRM

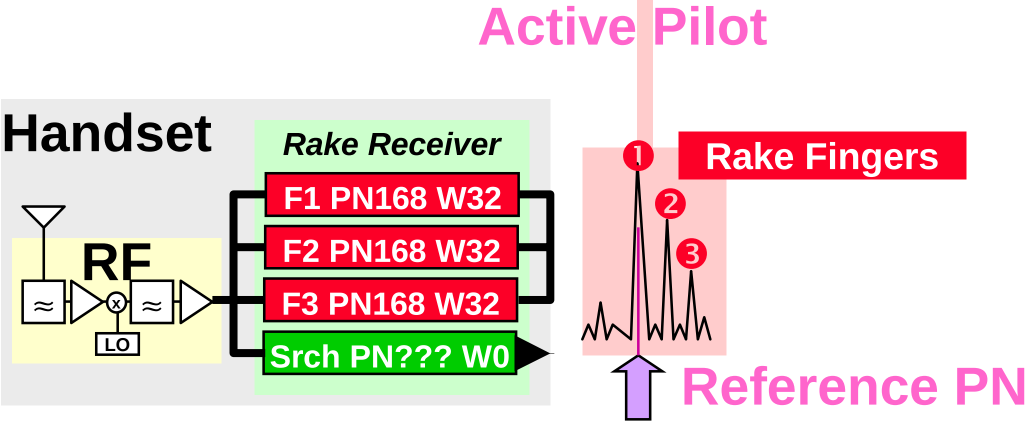


Find Strongest Pilot, Read Sync Channel



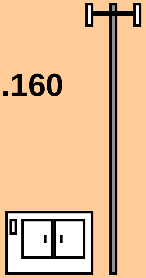
1. **Pilot Searcher Scans the Entire Range of PNs**

2. Put Rake finger(s) on strongest available PN, decode Walsh 32, and read Sync Channel Message



SYNC CHANNEL MESSAGE

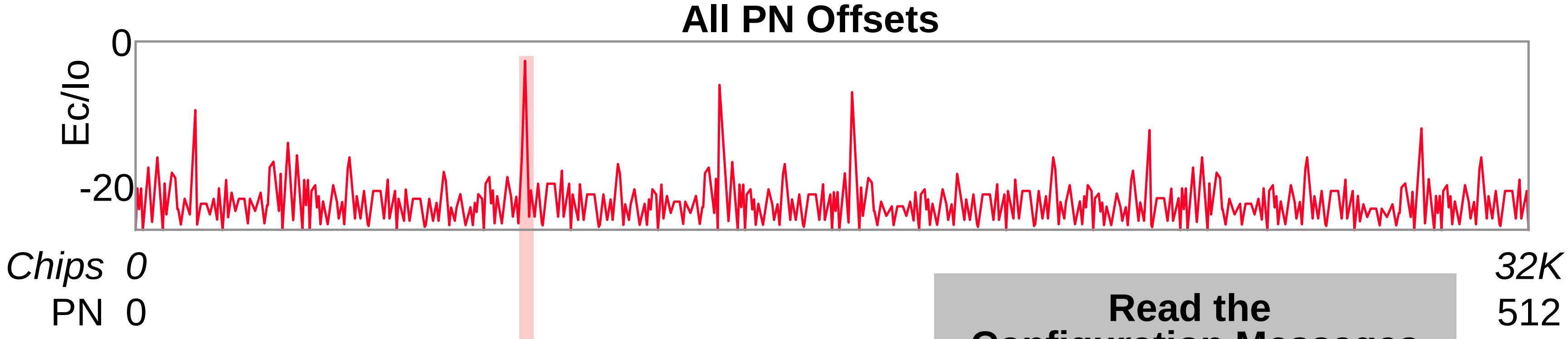
98/05/24 23:14:09.817 [SCH]
MSG_LENGTH = 208 bits
MSG_TYPE = Sync Channel Message
P_REV = 3
MIN_P_REV = 2
SID = 179
NID = 0
PILOT_PN = 168
Offset Index
LC_STATE = 0x0348D60E013
SYS_TIME = 98/05/24 23:14:10.160
LP_SEC = 12
LTM_OFF = -300 minutes
DAYLT = 0
PRAT = 9600 bps
RESERVED = 1



The Configuration Messages

- After reading the Sync Channel, the mobile is now capable of reading the Paging Channel, which it now monitors constantly
- Before it is allowed to transmit or operate on this system, the mobile must collect a complete set of configuration messages
- Collection is a short process -- all configuration messages are repeated on the paging channel every 1.28 seconds
- The configuration messages contain sequence numbers so the mobile can recognize if any of the messages have been freshly updated as it continues to monitor the paging channel
    - Access parameters message sequence number
    - Configuration message sequence number
    - If a mobile notices a changed sequence number, or if 600 seconds passes since the last time these messages were read, the mobile reads all of them again

Go to Paging Channel, Get Configured

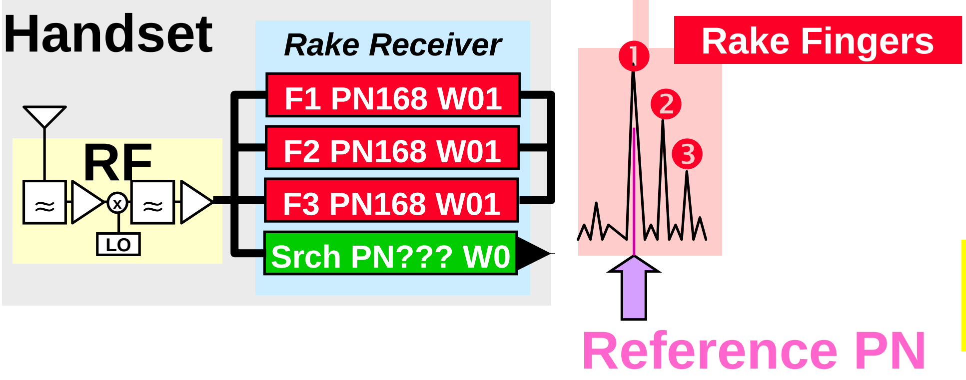


Keep Rake finger(s) on strongest available PN, decode Walsh 1, and monitor the Paging Channel

Active Pilot

Read the Configuration Messages

- Access Parameters Msg
- System Parameters Msg
- CDMA Channel List Msg
- Extended System Parameters Msg (*opt.)
- (Extended*) Neighbor List Msg
- Global Service Redirection Msg (*opt.)

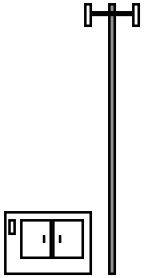


Now we're ready to operate!!

Two Very Important Configuration Messages

ACCESS PARAMETERS MESSAGE

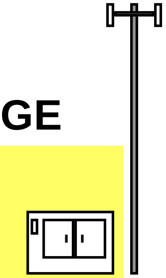
```
98/05/24 23:14:10.427 [PCH]
MSG_LENGTH = 184 bits
MSG_TYPE = Access Parameters Message
PILOT_PN = 168 Offset Index
ACC_MSG_SEQ = 27
ACC_CHAN = 1 channel
NOM_PWR = 0 dB INIT_PWR = 0 dB PWR_STEP = 4 dB
NUM_STEP = 5 Access Probes Maximum
MAX_CAP_SZ = 4 Access Channel Frames Maximum
PAM_SZ = 3 Access Channel Frames
Persist Val for Acc Overload Classes 0-9 = 0
Persist Val for Acc Overload Class 10 = 0
Persist Val for Acc Overload Class 11 = 0
Persist Val for Acc Overload Class 12 = 0
Persist Val for Acc Overload Class 13 = 0
Persist Val for Acc Overload Class 14 = 0
Persist Val for Acc Overload Class 15 = 0
Persistance Modifier for Msg Tx = 1
Persistance Modifier for Reg = 1
Probe Randomization = 15 PN chips
Acknowledgement Timeout = 320 ms
Probe Backoff Range = 4 Slots Maximum
Probe Sequence Backoff Range = 4 Slots Max.
Max # Probe Seq for Requests = 2 Sequences
Max # Probe Seq for Responses = 2 Sequences
Authentication Mode = 1
Random Challenge Value = Field Omitted
Reserved Bits = 99
```



SYSTEM PARAMETERS MESSAGE

```
98/05/24 23:14:11.126 [PCH] MSG_LENGTH = 264 bits
MSG_TYPE = System Parameters Message
PILOT_PN = 168 Offset Index
CONFIG_MSG_SEQ = 0
SID = 179     NID = 0
REG_ZONE = 0     TOTAL_ZONES = 0  ZONE_TIMER = 60 min
MULT_SIDS = 0    MULT_NID = 0  BASE_ID = 8710
BASE_CLASS = Public Macrocellular
PAGE_CHAN = 1 channel
MAX_SLOT_CYCLE_INDEX = 0
HOME_REG = 0  FOR_SID_REG = 0  FOR_NID_REG = 1
POWER_UP_REG = 0   POWER_DOWN_REG = 0
PARAMETER_REG = 1  REG_PRD = 0.08 sec
BASE_LAT = 00D00'00.00N  BASE_LONG = 000D00'00.00E
REG_DIST = 0
SRCH_WIN_A = 40 PN chips
SRCH_WIN_N = 80 PN chips
SRCH_WIN_R = 4 PN chips
NGHBR_MAX_AGE = 0
PWR_REP_THRESH = 2 frames
PWR_REP_FRAMES = 56 frames
PWR_THRESH_ENABLE = 1
PWR_PERIOD_ENABLE = 0
PWR_REP_DELAY = 20 frames
RESCAN = 0
T_ADD = -13.0 Db    T_DROP = -15.0 dB    T_COMP = 2.5 dB
T_TDROP = 4 sec
EXT_SYS_PARAMETER = 1
RESERVED = 0
GLOBAL_REDIRECT = 0
```

Four Additional Configuration Messages



CDMA CHANNEL LIST MESSAGE

```
98/05/24 23:14:10.786 [PCH]
MSG_LENGTH = 72 bits
MSG_TYPE = CDMA Channel List Message
PILOT_PN = 168 Offset Index
CONFIG_MSG_SEQ = 0
CDMA_FREQ = 283
RESERVED = Field Omitted
```

NEIGHBOR LIST

```
98/05/24 23:14:11.486 [PCH]
MSG_LENGTH = 216 bits
MSG_TYPE = Neighbor List Message
PILOT_PN = 168 Offset Index
CONFIG_MSG_SEQ = 0
PILOT_INC = 4 Offset Index
NGHBR_CONFIG = 0   NGHBR_PN = 220 Offset Index
NGHBR_CONFIG = 0   NGHBR_PN = 52 Offset Index
NGHBR_CONFIG = 0   NGHBR_PN = 500 Offset Index
NGHBR_CONFIG = 0   NGHBR_PN = 8 Offset Index
NGHBR_CONFIG = 0   NGHBR_PN = 176 Offset Index
NGHBR_CONFIG = 0   NGHBR_PN = 304 Offset Index
NGHBR_CONFIG = 0   NGHBR_PN = 136 Offset Index
NGHBR_CONFIG = 0   NGHBR_PN = 384 Offset Index
NGHBR_CONFIG = 0   NGHBR_PN = 216 Offset Index
NGHBR_CONFIG = 0   NGHBR_PN = 68 Offset Index
NGHBR_CONFIG = 0   NGHBR_PN = 328 Offset Index
NGHBR_CONFIG = 0   NGHBR_PN = 112 Offset Index
RESERVED = 0
```

EXTENDED SYSTEM PARAMETERS

```
98/05/24 23:14:10.946 [PCH]
MSG_LENGTH = 104 bits
MSG_TYPE = Extended System Parameters Message
PILOT_PN = 168 Offset Index
CONFIG_MSG_SEQ = 0  RESERVED = 0
PREF_MSID_TYPE = IMSI and ESN
MCC = 000    IMSI_11_12 = 00
RESERVED_LEN = 8 bits
RESERVED_OCTETS = 0x00
BCAST_INDEX = 0
RESERVED = 0
```

GLOBAL SERVICE REDIRECTION

```
98/05/17   24:21.566 Paging Channel: Global Service Redirection
PILOT_PN: 168, MSG_TYPE: 96, CONFIG_MSG_SEQ: 0
Redirected access overload classes:    { 0, 1 },
RETURN_IF_FAIL: 0,
DELETE_TMSI: 0,
Redirection to an analog system:
EXPECTED_SID = 0
Do not ignore CDMA Available indicator on the redirected analog
system
Attempt service on either System A or B with the custom system
selection process
```

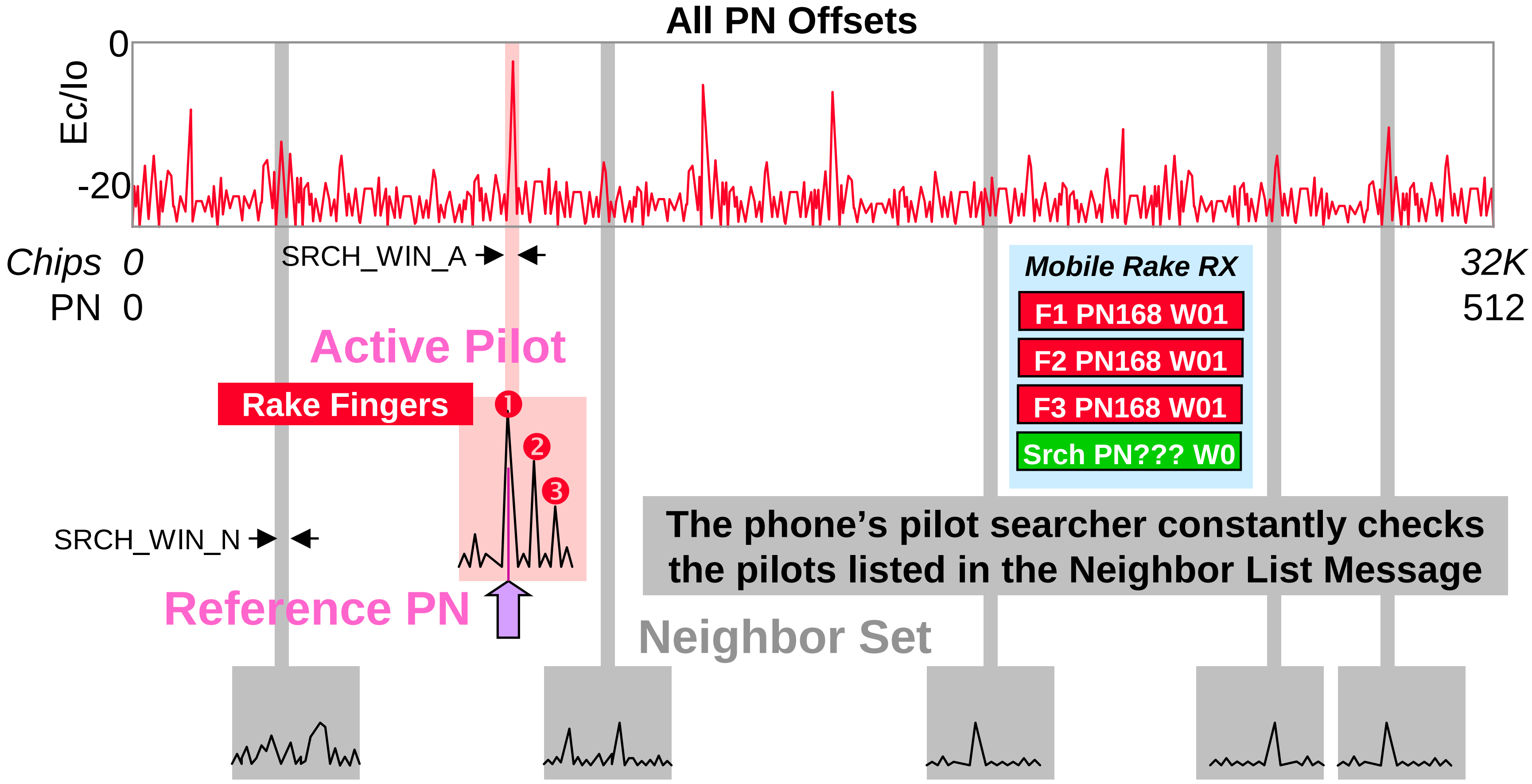
Example 2

Let’s do an
Idle Mode Handoff!

Idle Mode Handoff

- An idle mobile always demodulates the best available signal
  - In idle mode, it isn't possible to do soft handoff and listen to multiple sectors or base stations at the same time -- the paging channel information stream is different on each sector, not synchronous -- just like ABC, NBC, CBS, and CNN TV news programs aren't in word-sync for simultaneous viewing
  - Since a mobile can't combine signals, the mobile must switch quickly, always enjoying the best available signal
- The mobile's pilot searcher is constantly checking neighbor pilots
- If the searcher notices a better signal, the mobile continues on the current paging channel until the end of the current superframe, then instantly switches to the paging channel of the new signal
  - The system doesn't know the mobile did this! (Does NBC's Tom Brokaw know you just switched your TV to CNN?)
- On the new paging channel, if the mobile learns that registration is required, it re-registers on the new sector

Idle Mode on the Paging Channel: Meet the Neighbors, track the Strongest Pilot

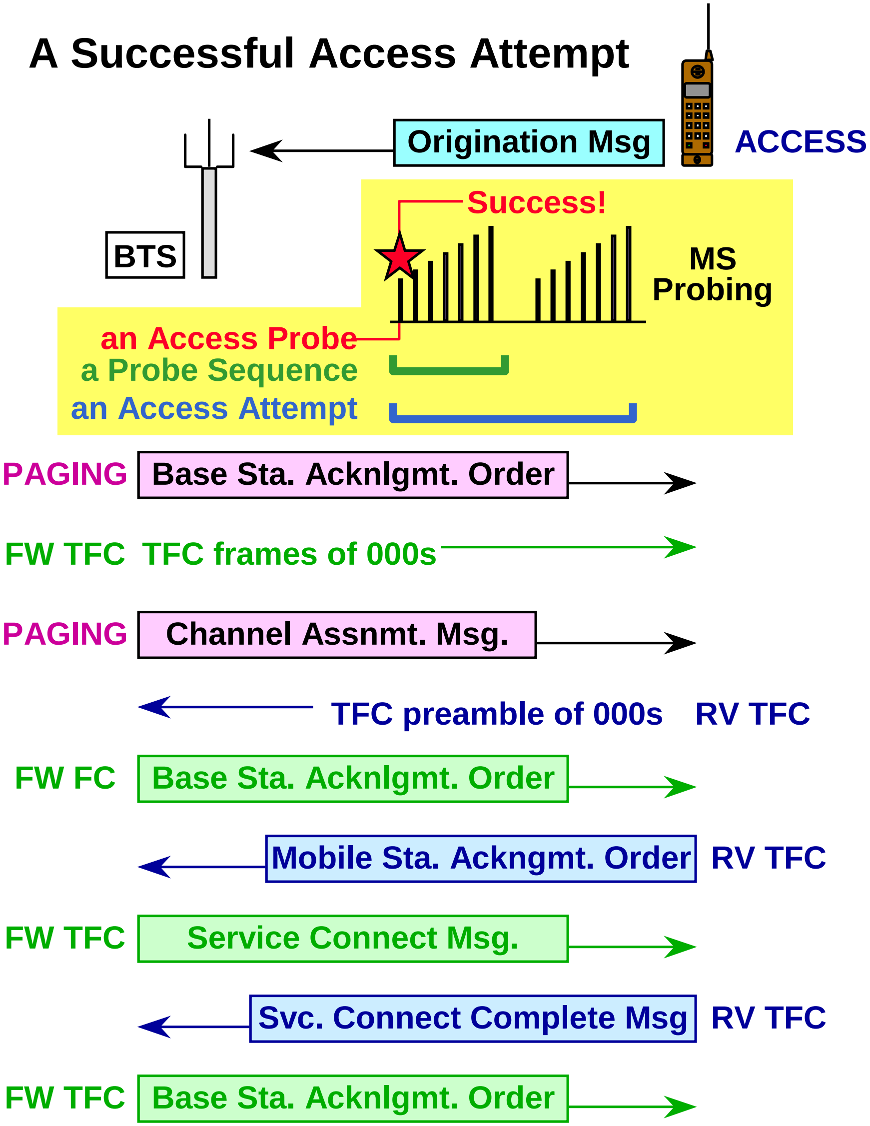


The phone's pilot searcher constantly checks the pilots listed in the Neighbor List Message

If the searcher ever notices a neighbor pilot substantially stronger than the current reference pilot, it becomes the new reference pilot and the phone switches over to its paging channel on the next superframe. This is called an *idle mode handoff*.

Phone Operation on the Access Channel

- A sector's Paging Channel announces 1 (typ) to 32 (max) Access Channels: PN Long Code offsets for mobiles to use if accessing the system.
  - For mobiles sending Registration, Origination, Page Responses
  - Base Station always listening!
- On the access channel, phones are not yet under BTS closed-loop power control!
- Phones access the BTS by "probing" at power levels determined by receive power and an open loop formula
  - If "probe" not acknowledged by BTS within ACC_TMO (~400 mS.), phone will wait a random time (~200 mS) then probe again, stronger by PI db.
  - There can be 15 max. (typ. 5) probes in a sequence and 15 max. (typ. 2) sequences in an access attempt
  - most attempts succeed on first probe!
- The Access Parameters message on the paging channel announces values of all related parameters



Call is Established!

Example 3

Let’s Register!

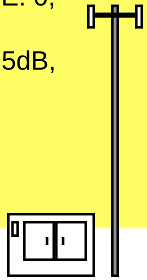
Registration

- Registration is the process by which an idle mobile lets the system know it’s awake and available for incoming calls
  - this allows the system to inform the mobile’s home switch of the mobile’s current location, so that incoming calls can be delivered
  - registration also allows the system to intelligently page the mobile only in the area where the mobile is currently located, thereby eliminating useless congestion on the paging channels in other areas of the system
- There are many different conditions that could trigger an obligation for the mobile to register
  - there are flags in the System Parameters Message which tell the mobile when it must register on the current system

An Actual Registration

SYSTEM PARAMETERS MESSAGE

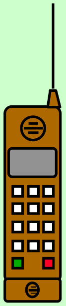
```
18:26.826 [PCH] System Parameters Message
Pilot_PN: 32
CONFIG_MSG_SEQ: 14      SID: 16420       NID: 0,
REG_ZONE: 0     TOTAL_ZONES: 0   Zone timer length (min): 1
MULT_SIDS: 0    MULT_NIDS: 0
BASE_ID: 1618   BASE_CLASS: Reserved
PAG_CHAN: 1    MAX_SLOT_CYCLE_INDEX: 2
HOME_REG: 1      FOR_SID_REG: 1      FOR_NID_REG: 1,
POWER_UP_REG: 1     POWER_DOWN_REG: 1
PARAMETER_REG: 1    Registration period (sec): 54
Base station   0°00´00.00¨ Lon., 0°00´00.00° Lat.  REG_DIST: 0
SRCH_WIN_A (PN chips): 28      SRCH_WIN_N (PN chips): 100,
SRCH_WIN_R (PN chips): 130    NGHBR_MAX_AGE: 2
PWR_REP_THRESH: 2          PWR_REP_FRAMES (frames): 15
PWR_THRESH_ENABLE: 1   PWR_PERIOD_ENABLE: 0,
PWR_REP_DELAY: 1 (4 frames)     RESCAN: 0,
T_ADD: -14.0dB      T_DROP: -16.0dB      T_COMP: 2.5dB,
T_TDROP: 4s
EXT_SYS_PARAMETER: 1
EXT_NGHBR_LIST: 1
GLOBAL_REDIRECT: 0
```



The System Parameters Message tells all mobiles when they should register. This mobile notices that it is obligated to register, so it transmits a Registration Message.

REGISTRATION MESSAGE

```
16:18:27.144 Access Channel: Registration
ACK_SEQ: 7  MSG_SEQ: 1  ACK_REQ: 1  VALID_ACK: 0
ACK_TYPE: 0
MSID_TYPE: 3,  ESN: [0x 01 99 0d fc]
MFR 1, Reserved 38, Serial Number 69116,
IMSI: (Class: 0, Class_0_type: 1)  [0x 01 8d 31 74 29 36]
00-416-575-0421
AUTH_MODE: 0
REG_TYPE: Timer-based
SLOT_CYCLE_INDEX: 2
MOB_P_REV: 1
EXT_SCM: 1
SLOTTED_MODE: 1
MOB_TERM: 1
```



BASE STATION ACKNOWLEDGMENT

```
16:18:27.506 Paging Channel: Order
ACK_SEQ: 1    MSG_SEQ: 0    ACK_REQ: 0    VALID_ACK: 1
MSID_TYPE: 2    IMSI: (Class: 0, Class_0_type: 3)
[0x 02 47 8d 31 74 29 36]   (302) 00-416-575-0421
Order type: Base Station Acknowledgement Order
```

The base station confirms that the mobile's registration message was received. We're officially registered!

Example 4

Let’s Receive an incoming Call!

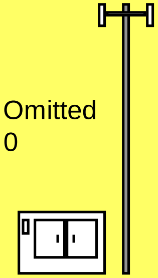
Receiving an Incoming Call

- All idle mobiles monitor the paging channel to receive incoming calls.
- When an incoming call appears, the paging channel notifies the mobile in a General Page Message.
- A mobile which has been paged sends a Page Response Message on the access channel.
- The system sets up a traffic channel for the call, then notifies the mobile to use it with a Channel Assignment Message.
- The mobile and the base station notice each other’s traffic channel signals and confirm their presence by exchanging acknowledgment messages.
- The base station and the mobile negotiate what type of call this will be -- I.e., 13k voice, etc.
- The mobile is told to ring and given a “calling line ID” to display.
- When the human user presses the send button, the audio path is completed and the call proceeds.

An Actual Page and Page Response

GENERAL PAGE MESSAGE

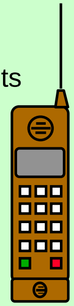
```
98/05/24 23:14:46.127 [PCH] General Page Message
MSG_LENGTH = 128 bits
MSG_TYPE = General Page Message
CONFIG_MSG_SEQ = 1       ACC_MSG_SEQ = 20
CLASS_0_DONE = 1
CLASS_1_DONE = 1          RESERVED = 0
BROADCAST_DONE = 1      RESERVED = 0
ADD_LENGTH = 0 bits        ADD_PFIELD = Field Omitted
PAGE_CLASS = 0               PAGE_SUBCLASS = 0
MSG_SEQ = 1
IMSI_S = 6153300644
SPECIAL_SERVICE = 1
SERVICE_OPTION = 32768
RESERVED = Field Omitted
```



The system pages the mobile,
615-330-0644.

PAGE RESPONSE MESSAGE

```
98/05/24 23:14:46.425 [ACH] Page Response Message
MSG_LENGTH = 216 bits
MSG_TYPE = Page Response Message
ACK_SEQ = 1     MSG_SEQ = 2    ACK_REQ = 1
VALID_ACK = 1   ACK_TYPE = 2
MSID_TYPE = IMSI and ESN         MSID_LEN = 9 octets
ESN = 0xD30E415C       IMSI_CLASS = 0
IMSI_CLASS_0_TYPE = 0     RESERVED = 0
IMSI_S = 6153300644
AUTH_MODE = 1
AUTHR = 0x307B5       RANDC = 0xC6      COUNT = 0
MOB_TERM = 1          SLOT_CYCLE_INDEX = 0
MOB_P_REV = 3         SCM = 106
REQUEST_MODE = Either Wide Analog or CDMA Only
SERVICE_OPTION = 32768      PM = 0
NAR_AN_CAP = 0       RESERVED = 0
```



The mobile responds to the page.

BASE STATION ACKNOWLEDGMENT

```
98/05/24 23:14:46.768 [PCH] Order Message
MSG_LENGTH = 112 bits
MSG_TYPE = Order Message
ACK_SEQ = 2    MSG_SEQ = 0    ACK_REQ = 0
VALID_ACK = 1
ADDR_TYPE = IMSI      ADDR_LEN = 40 bits
IMSI_CLASS = 0   IMSI_CLASS_0_TYPE = 0    RESERVED = 0
IMSI_S = 6153300644
ORDER = Base Station Acknowledgement Order
ADD_RECORD_LEN = 0 bits
Order-Specific Fields = Field Omitted       RESERVED = 0
```

The base station confirms that the mobile's page response was received. Now the mobile is waiting for channel assignment, expecting a response within 12 seconds.

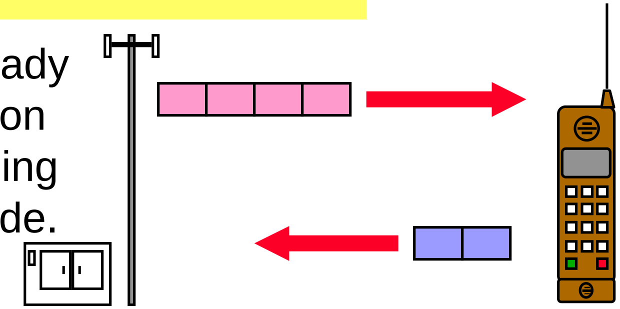
Channel Assignment and Traffic Channel Confirmation

CHANNEL ASSIGNMENT MESSAGE

```
18:14:47.027 Paging Channel: Channel Assignment
ACK_SEQ: 2     MSG_SEQ: 1    ACK_REQ: 0     VALID_ACK: 1
MSID_TYPE: 2    IMSI: (Class: 0, Class_0_type: 0)
[0x 01 f8 39 6a 15] 615-330-0644
ASSIGN_MODE: Traffic Channel Assignment
ADD_RECORD_LEN: 5   FREQ_INCL: 1   GRANTED_MODE: 2
CODE_CHAN: 43    FRAME_OFFSET: 2
ENCRYPT_MODE: Encryption disabled
BAND_CLASS: 800 MHz cellular band
CDMA_FREQ: 283
```

Only about 400 ms. after the base station acknowledgment order, the mobile receives the channel assignment message.

The base station is already sending blank frames on the forward channel,using the assigned Walsh code.



The mobile sees at least two good blank frames in a row on the forward channel, and concludes this is the right traffic channel. It sends a preamble of two blank frames of its own on the reverse traffic channel.

BASE STATION ACKNOWLEDGMENT

```
18:14:47.581 Forward Traffic Channel: Order
ACK_SEQ: 7     MSG_SEQ: 0     ACK_REQ: 1
ENCRYPTION: 0     USE_TIME: 0     ACTION_TIME: 0
Base Station Acknowledgement Order
```

The base station acknowledges receiving the mobile’s preamble.

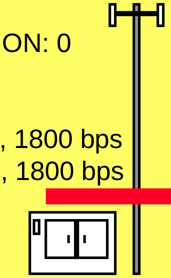
MOBILE STATION ACKNOWLEDGMENT

```
18:14:47.598 Reverse Traffic Channel: Order
ACK_SEQ: 0   MSG_SEQ: 0   ACK_REQ: 0
ENCRYPTION: 0
Mobile Station Acknowledgement Order
```

The mobile station acknowledges the base station’s acknowledgment. Everybody is ready!

Service Negotiation and Mobile Alert

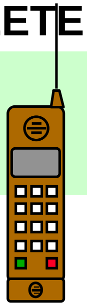
SERVICE CONNECT MESSAGE



18:14:47.760 Forward Traffic Channel: Service Connect
ACK_SEQ: 0   MSG_SEQ: 1   ACK_REQ: 0   ENCRYPTION: 0
USE_TIME: 0   ACTION_TIME: 0   SERV_CON_SEQ: 0
Service Configuration: supported Transmission:
Forward Traffic Channel Rate (Set 2): 14400, 7200, 3600, 1800 bps
Reverse Traffic Channel Rate (Set 2): 14400, 7200, 3600, 1800 bps
Service option: (6) Voice (13k) (0x8000)
Forward Traffic Channel: Primary Traffic
Reverse Traffic Channel: Primary Traffic

Now that both sides have arrived on the traffic channel, the base station proposes that the requested call actually begin.

SERVICE CONNECT COMPLETE MSG.



18:14:47.835 Reverse Traffic Channel:
Service Connect Completion
ACK_SEQ: 1   MSG_SEQ: 3   ACK_REQ: 1
ENCRYPTION: 0   SERV_CON_SEQ: 0

The mobile agrees and says its ready to play.

ALERT WITH INFORMATION MESSAGE

18:14:47.961 Forward Traffic Channel:
Alert With Information
ACK_SEQ: 3   MSG_SEQ: 1   ACK_REQ: 1   ENCRYPTION: 0
SIGNAL_TYPE = IS-54B Alerting
ALERT_PITCH = Medium Pitch (Standard Alert)
SIGNAL = Long   RESERVED = 0
RECORD_TYPE = Calling Party Number
RECORD_LEN = 96 bits
NUMBER_TYPE = National Number
NUMBER_PLAN = ISDN/Telephony Numbering Plan
PI = Presentation Allowed   SI = Network Provided
CHARi = 6153000124   RESERVED = 0   RESERVED = 0

The base station orders the mobile to ring, and gives it the calling party's number to display.

SERVICE CONNECT COMPLETE is a major milestone in call processing. Up until now, this was an access attempt. Now it is officially a call.

18:14:48.018 Reverse Traffic Channel: Order
ACK_SEQ: 1   MSG_SEQ: 4   ACK_REQ: 0
ENCRYPTION: 0
Mobile Station Acknowledgement Order

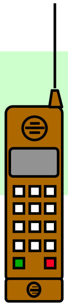
The mobile says it's ringing.

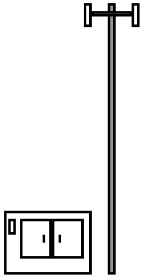
The Human Answers! Connect Order

The mobile has been ringing for several seconds. The human user finally comes over and presses the send button to answer the call.

CONNECT ORDER

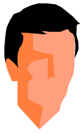
18:14:54.758 Reverse Traffic Channel: Order
ACK_SEQ: 6   MSG_SEQ: 0   ACK_REQ: 1
ENCRYPTION: 0
Connect Order



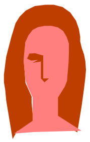


BASE STATION ACKNOWLEDGMENT

18:14:54.920 Forward Traffic Channel: Order
ACK_SEQ: 0   MSG_SEQ: 1   ACK_REQ: 0
ENCRYPTION: 0   USE_TIME: 0   ACTION_TIME: 0
Base Station Acknowledgement Order



Now the switch completes the audio circuit and the two callers can talk!



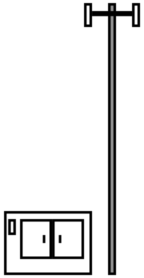
Example 5

Let's make an Outgoing Call!

Placing an Outgoing Call

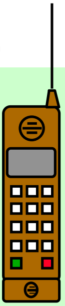
- The mobile user dials the desired digits, and presses SEND.
- Mobile transmits an Origination Message on the access channel.
- The system acknowledges receiving the origination by sending a base station acknowledgement on the paging channel.
- The system arranges the resources for the call and starts transmitting on the traffic channel.
- The system notifies the mobile in a Channel Assignment Message on the paging channel.
- The mobile arrives on the traffic channel.
- The mobile and the base station notice each other’s traffic channel signals and confirm their presence by exchanging acknowledgment messages.
- The base station and the mobile negotiate what type of call this will be -- I.e., 13k voice, etc.
- The audio circuit is completed and the mobile caller hears ringing.

Origination



The mobile sends an origination message on the access channel.

ORIGINATION MESSAGE



```
17:48:53.144 Access Channel: Origination
ACK_SEQ: 7   MSG_SEQ: 6   ACK_REQ: 1
VALID_ACK: 0   ACK_TYPE: 0   MSID_TYPE: 3
ESN: [0x 00 06 98 24] MFR 0   Reserved 1
Serial Number 170020
IMSI: (Class: 0, Class_0_type: 0)
[0x 03 5d b8 97 c2] 972-849-5073
AUTH_MODE: 0    MOB_TERM: 1
SLOT_CYCLE_INDEX: 2    MOB_P_REV: 1   EXT_SCM: 1
DualMode: 0    SLOTTED_MODE: 1    PowerClass: 0
REQUEST_MODE: CDMA only   SPECIAL_SERVICE: 1
Service option: (6) Voice (13k) (0x8000)     PM: 0
DIGIT_MODE: 0   MORE_FIELDS: 0   NUM_FIELDS: 11
Chari: 18008900829
NAR_AN_CAP: 0
```

BASE STATION ACKNOWLEDGMENT

```
17:48:53.487 Paging Channel: Order
ACK_SEQ: 6   MSG_SEQ: 0   ACK_REQ: 0   VALID_ACK: 1
MSID_TYPE: 2
IMSI: (Class: 0, Class_0_type: 0)
[0x 03 5d b8 97 c2]   972-849-5073
Base Station Acknowledgment Order
```

The base station confirms that the origination message was received.

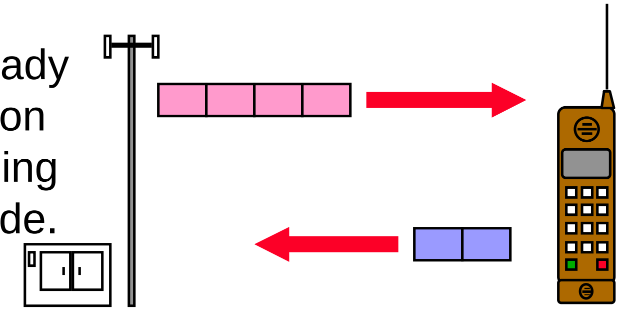
CHANNEL ASSIGNMENT MESSAGE

```
17:48:54.367 Paging Channel: Channel Assignment
ACK_SEQ: 6   MSG_SEQ: 1   ACK_REQ: 0   VALID_ACK: 1
MSID_TYPE: 2
IMSI: (Class: 0, Class_0_type: 0)
[0x 03 5d b8 97 c2] 972-849-5073
ASSIGN_MODE: Traffic Channel Assignment,
ADD_RECORD_LEN: 5   FREQ_INCL: 1   GRANTED_MODE: 2
CODE_CHAN: 12   FRAME_OFFSET: 0
ENCRYPT_MODE:  Encryption disabled
BAND_CLASS: 1.8 to 2.0 GHz PCS band
CDMA_FREQ: 425
```

The base station sends a Channel Assignment Message and the mobile goes to the traffic channel.

Traffic Channel Confirmation

The base station is already sending blank frames on the forward channel,using the assigned Walsh code.



The mobile sees at least two good blank frames in a row on the forward channel, and concludes this is the right traffic channel. It sends a preamble of two blank frames of its own on the reverse traffic channel.

BASE STATION ACKNOWLEDGMENT

```
17:48:54.757 Forward Traffic Channel: Order
ACK_SEQ: 7   MSG_SEQ: 0   ACK_REQ: 1   ENCRYPTION: 0
USE_TIME: 0   ACTION_TIME: 0
Base Station Acknowledgment Order
```

The base station acknowledges receiving the mobile’s preamble.

MOBILE STATION ACKNOWLEDGMENT

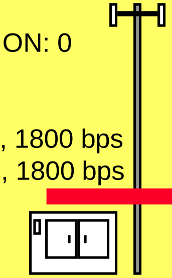
```
17:48:54.835 Reverse Traffic Channel: Order
ACK_SEQ: 0   MSG_SEQ: 0   ACK_REQ: 0
ENCRYPTION: 0
Mobile Station Acknowledgment Order
```

The mobile station acknowledges the base station’s acknowledgment. Everybody is ready!

Service Negotiation and Connect Complete

SERVICE CONNECT MESSAGE

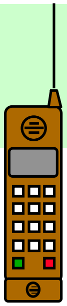
17:48:55.098 Forward Traffic Channel: Service Connect
ACK_SEQ: 7   MSG_SEQ: 1   ACK_REQ: 1   ENCRYPTION: 0
USE_TIME: 0   ACTION_TIME: 0   SERV_CON_SEQ: 0
Service Configuration   Supported Transmission:
Forward Traffic Channel Rate (Set 2): 14400, 7200, 3600, 1800 bps
Reverse Traffic Channel Rate (Set 2): 14400, 7200, 3600, 1800 bps
Service option: (6) Voice (13k) (0x8000)
Forward Traffic Channel: Primary Traffic
Reverse Traffic Channel: Primary Traffic



Now that the traffic channel is working in both directions, the base station proposes that the requested call actually begin.

SERVICE CONNECT COMPLETE MSG.

17:48:55.137 Reverse Traffic Channel: Service Connect Completion ACK_SEQ: 1, MSG_SEQ: 0, ACK_REQ: 1, ENCRYPTION: 0,   SERV_CON_SEQ: 0



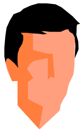
The mobile agrees and says its ready to play.

BASE STATION ACKNOWLEDGMENT

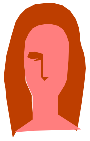
17:48:55.779 Forward Traffic Channel: Order
ACK_SEQ: 0   MSG_SEQ: 0   ACK_REQ: 0   ENCRYPTION: 0
USE_TIME: 0   ACTION_TIME: 0
Base Station Acknowledgment Order

The base station agrees.

SERVICE CONNECT COMPLETE is a major milestone in call processing. Up until now, this was an access attempt. Now it is officially a call.



Now the switch completes the audio circuit and the two callers can talk!



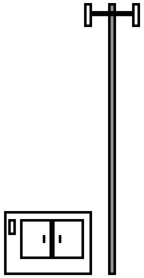
Example 6

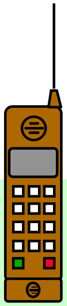
Let’s End a Call!

Ending A Call

- A normal call continues until one of the parties hangs up. That action sends a Release Order, “normal release”.
- The other side of the call sends a Release Order, “no reason given”.
  - *If a normal release is visible, the call ended normally*.
- At the conclusion of the call, the mobile reacquires the system.
  - Searches for the best pilot on the present CDMA frequency
  - Reads the Sync Channel Message
  - Monitors the Paging Channel steadily
- Several different conditions can cause a call to end abnormally:
  - the forward link is lost at the mobile, and a fade timer acts
  - the reverse link is lost at the base station, and a fade timer acts
  - a number of forward link messages aren’t acknowledged, and the base station acts to tear down the link
  - a number of reverse link messages aren’t acknowledged, and the mobile station acts to tear down the link

A Beautiful End to a Normal Call





MOBILE RELEASE ORDER

```
17:49:21.715 Reverse Traffic Channel: Order
ACK_SEQ: 1   MSG_SEQ: 1   ACK_REQ: 1
ENCRYPTION: 0
Release Order (normal release)
```

At the end of a normal call, this mobile user pressed end.

BASE STATION ACKNOWLEDGMENT

```
17:49:21.936 Forward Traffic Channel: Order
ACK_SEQ: 1   MSG_SEQ: 2   ACK_REQ: 0   ENCRYPTION: 0,
USE_TIME: 0   ACTION_TIME: 0
Base Station Acknowledgement Order
```

BASE STATION RELEASE ORDER

```
17:49:21.997 Forward Traffic Channel: Order
ACK_SEQ: 1   MSG_SEQ: 3   ACK_REQ: 0   ENCRYPTION: 0
USE_TIME: 0   ACTION_TIME: 0
Release Order (no reason given)
```

The base station acknowledged receiving the message, then sent a release message of its own.

SYNC CHANNEL MESSAGE

```
17:49:22.517 Sync Channel
MSG_TYPE: 1   Sync Channel Message
P_REV: 1   MIN_P_REV: 1
SID: 4112        NID: 2        Pilot_PN: 183
LC_STATE: 0x318fe5d84a5
SYS_TIME: 0x1ae9683dc
LP_SEC: 9      LTM_OFF: -10    DAYLT: 1
Paging Channel Data Rate: 9600
CDMA_FREQ: 425
```

The mobile left the traffic channel, scanned to find the best pilot, and read the Sync Channel Message.

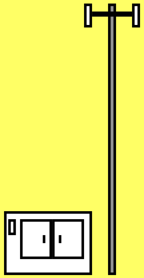
Example 7

Let’s receive Notification of a Voice Message!

Feature Notification

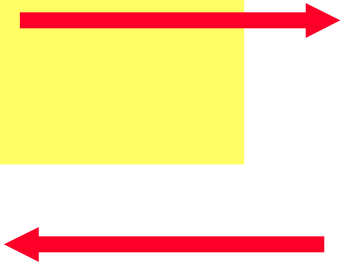
FEATURE NOTIFICATION MESSAGE

```
98/06/30 21:16:44.368 [PCH] Feature Notification Message
MSG_LENGTH = 144 bits
MSG_TYPE = Feature Notification Message
ACK_SEQ = 0
MSG_SEQ = 0
ACK_REQ = 1
VALID_ACK = 0
ADDR_TYPE = IMSI
ADDR_LEN = 56 bits
IMSI_CLASS = 0
IMSI_CLASS_0_TYPE = 3
RESERVED = 0
MCC = 302
IMSI_11_12 = 00
IMSI_S = 9055170325
RELEASE = 0
RECORD_TYPE = Message Waiting
RECORD_LEN = 8 bits
MSG_COUNT = 1
RESERVED = 0
```



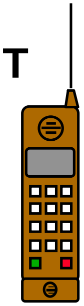
The Feature Notification Message on the Paging Channel tells a specific mobile it has voice messages waiting.

There are other record types to notify the mobile of other features.



MOBILE STATION ACKNOWLEDGMENT

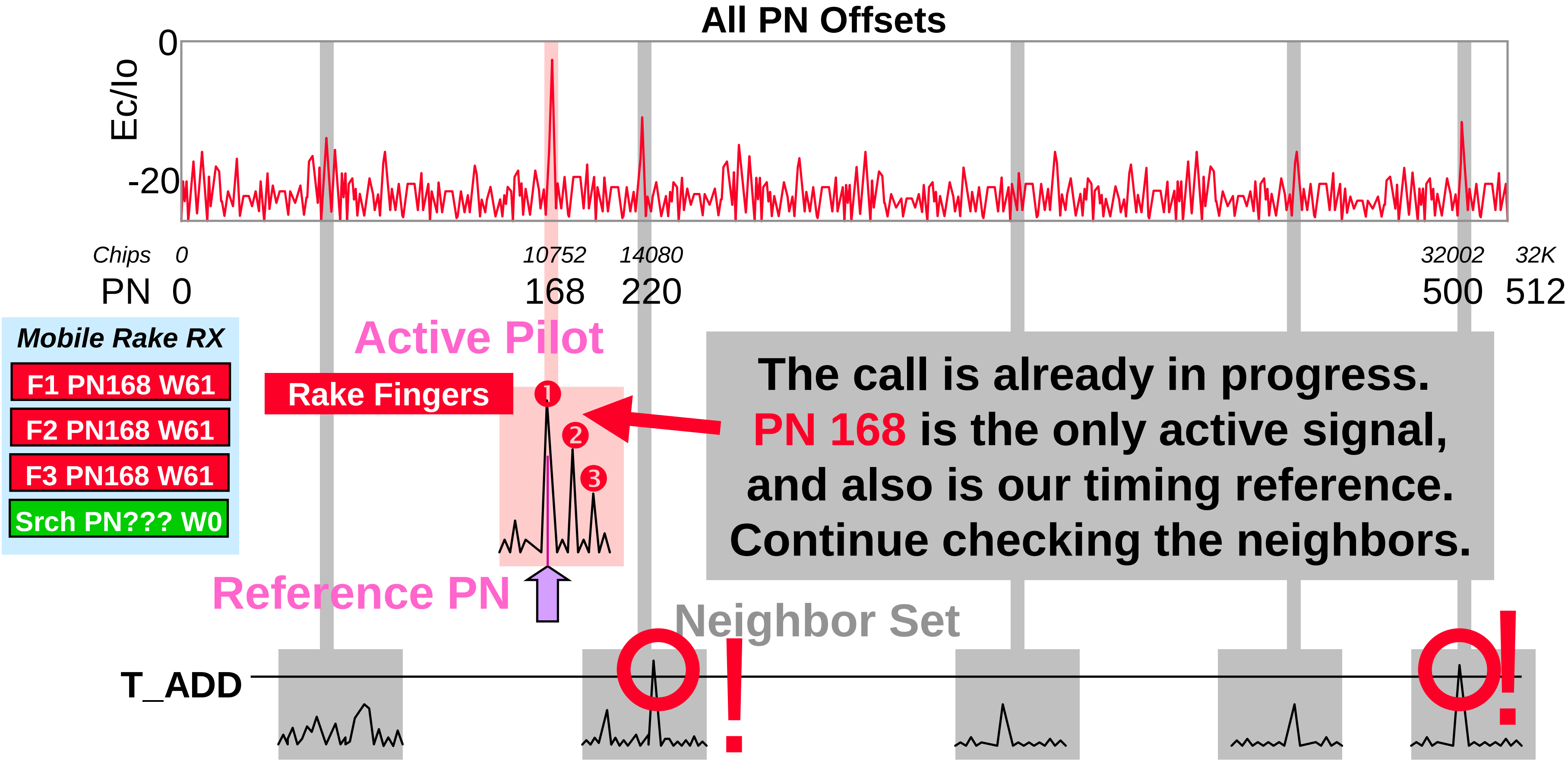
The mobile confirms it has received the notification by sending a Mobile Station Acknowledgment Order on the access channel.



Example 8

Let’s do a Handoff!

The Call is Already Established. What Next?



The call is already in progress.
PN 168 is the only active signal,
and also is our timing reference.
Continue checking the neighbors.

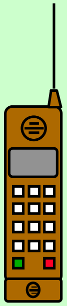
If we ever notice a neighbor with Ec/Io above T_ADD,
ask to use it!   Send a Pilot Strength Measurement Message!

Mobile Requests the Handoff!

Just prior to this message, this particular mobile already was in handoff with PN 168 and 220.
This pilot strength measurement message reports PN 500 has increased above T_Add, and the mobile wants to use it too.

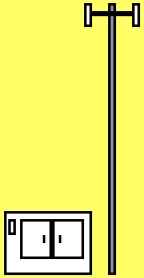
PILOT STRENGTH MEASUREMENT MESSAGE

98/05/24 23:14:02.205 [RTC]
Pilot Strength Measurement Message
MSG_LENGTH = 128 bits
MSG_TYPE = Pilot Strength Measurement Message
ACK_SEQ = 5 **MSG_SEQ = 0** ACK_REQ = 1
ENCRYPTION = Encryption Mode Disabled
REF_PN = 168 Offset Index (the Reference PN)
PILOT_STRENGTH = -6.0 dB
KEEP = 1
PILOT_PN_PHASE = 14080 chips (PN220+0chips)
PILOT_STRENGTH = -12.5 dB
KEEP = 1
PILOT_PN_PHASE = 32002 chips (PN500 + 2 chips)
PILOT_STRENGTH = -11.0 dB
KEEP = 1
RESERVED = 0



BASE STATION ACKNOWLEDGMENT

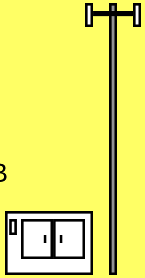
98/05/24 23:14:02.386 [FTC] Order Message
MSG_LENGTH = 64 bits
MSG_TYPE = Order Message
ACK_SEQ = 0 MSG_SEQ = 0 ACK_REQ = 0
ENCRYPTION = Encryption Mode Disabled
USE_TIME = 0 ACTION_TIME = 0
ORDER = Base Station Acknowledgment Order
ADD_RECORD_LEN = 0 bits
Order-Specific Fields = Field Omitted
RESERVED = 0



The base station acknowledges receiving the Pilot Strength Measurement Message.

System Authorizes the Handoff!

HANDOFF DIRECTION MESSAGE

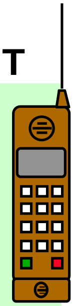


```
98/05/24 23:14:02.926 [FTC] Extended Handoff Direction Message
MSG_LENGTH = 136 bits
MSG_TYPE = Extended Handoff Direction Message
ACK_SEQ = 0  MSG_SEQ = 6  ACK_REQ = 1
ENCRYPTION = Encryption Mode Disabled
USE_TIME = 0  ACTION_TIME = 0  HDM_SEQ = 0
SEARCH_INCLUDED = 1
SRCH_WIN_A = 40 PN chips
T_ADD = -13.0 dB   T_DROP = -15.0 dB   T_COMP = 2.5 dB
T_TDROP = 4 sec
HARD_INCLUDED = 0 FRAME_OFFSET = Field Omitted
PRIVATE_LCM = Field Omitted  RESET_L2 = Field Omitted
RESET_FPC = Field Omitted  RESERVED = Field Omitted
ENCRYPT_MODE = Field Omitted  RESERVED = Field Omitted
NOM_PWR = Field Omitted  NUM_PREAMBLE = Field Omitted
BAND_CLASS = Field Omitted  CDMA_FREQ = Field Omitted
ADD_LENGTH = 0
PILOT_PN = 168    PWR_COMB_IND = 0    CODE_CHAN = 61
PILOT_PN = 220    PWR_COMB_IND = 1    CODE_CHAN = 20
PILOT_PN = 500    PWR_COMB_IND = 0    CODE_CHAN = 50
RESERVED = 0
```

The base station sends a Handof Direction Message authorizing the mobile to begin soft handoff with all three requested PNs. The pre-existing link on PN 168 will continue to use Walsh code 61, the new link on PN220 will use Walsh Code 20, and the new link on PN500 will use Walsh code 50.

The mobile acknowledges it has received the Handoff Direction Message.

MOBILE STATION ACKNOWLEDGMENT



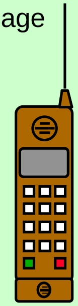
```
98/05/24 23:14:02.945 [RTC] Order Message
MSG_LENGTH = 56 bits     MSG_TYPE = Order Message
ACK_SEQ = 6   MSG_SEQ = 6   ACK_REQ = 0
ENCRYPTION = Encryption Mode Disabled
ORDER = Mobile Station Acknowledgment Order
ADD_RECORD_LEN = 0 bits
Order-Specific Fields = Field Omitted   RESERVED = 0
```

Mobile Implements the Handoff!

The mobile searcher quickly re-checks all three PNs. It still hears their pilots! The mobile sends a Handoff Completion Message, confirming it still wants to go ahead with the handoff.

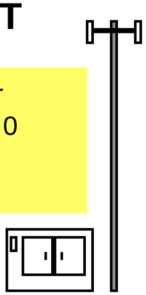
HANDOFF COMPLETION MESSAGE

```
98/05/24 23:14:02.985 [RTC] Handoff Completion Message
MSG_LENGTH = 72 bits
MSG_TYPE = Handoff Completion Message
ACK_SEQ = 6  MSG_SEQ = 1  ACK_REQ = 1
ENCRYPTION = Encryption Mode Disabled
LAST_HDM_SEQ = 0
PILOT_PN = 168 Offset Index
PILOT_PN = 220 Offset Index
PILOT_PN = 500 Offset Index
RESERVED = 0
```



BASE STATION ACKNOWLEDGMENT

```
98/05/24 23:14:03.085 [FTC] Forward Traffic Channel: Order
ACK_SEQ: 0   MSG_SEQ: 1  ACK_REQ: 0  ENCRYPTION: 0
USE_TIME: 0   ACTION_TIME: 0
Base Station Acknowledgement Order
```

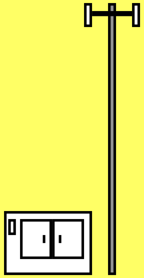


The base station confirms it has received the mobile's Handoff Completion message, and will continue with all of the links active.

Neighbor List Updated, Handoff is Complete!

NEIGHBOR LIST UPDATE MESSAGE

```
98/05/24 23:14:03.166 [FTC] Neighbor List Update Message
MSG_LENGTH = 192 bits
MSG_TYPE = Neighbor List Update Message
ACK_SEQ = 1  MSG_SEQ = 7  ACK_REQ = 1
ENCRYPTION = Encryption Mode Disabled
PILOT_INC = 4 Offset Index
NGHBR_PN = 164 Offset Index
NGHBR_PN = 68 Offset Index
NGHBR_PN = 52 Offset Index
NGHBR_PN = 176 Offset Index
NGHBR_PN = 304 Offset Index
NGHBR_PN = 136 Offset Index
NGHBR_PN = 112 Offset Index
NGHBR_PN = 372 Offset Index
NGHBR_PN = 36 Offset Index
NGHBR_PN = 8 Offset Index
NGHBR_PN = 384 Offset Index
NGHBR_PN = 216 Offset Index
NGHBR_PN = 328 Offset Index
NGHBR_PN = 332 Offset Index
NGHBR_PN = 400 Offset Index
NGHBR_PN = 96 Offset Index
RESERVED = 0
```

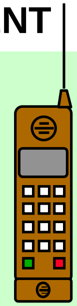


In response to the mobile’s Handoff Completion Message, the base station assembles a new *composite* neighbor list including all the neighbors of each of the three active pilots.

This is necessary since the mobile could be traveling toward any one of these pilots and may need to request soft handoff with any of them soon.

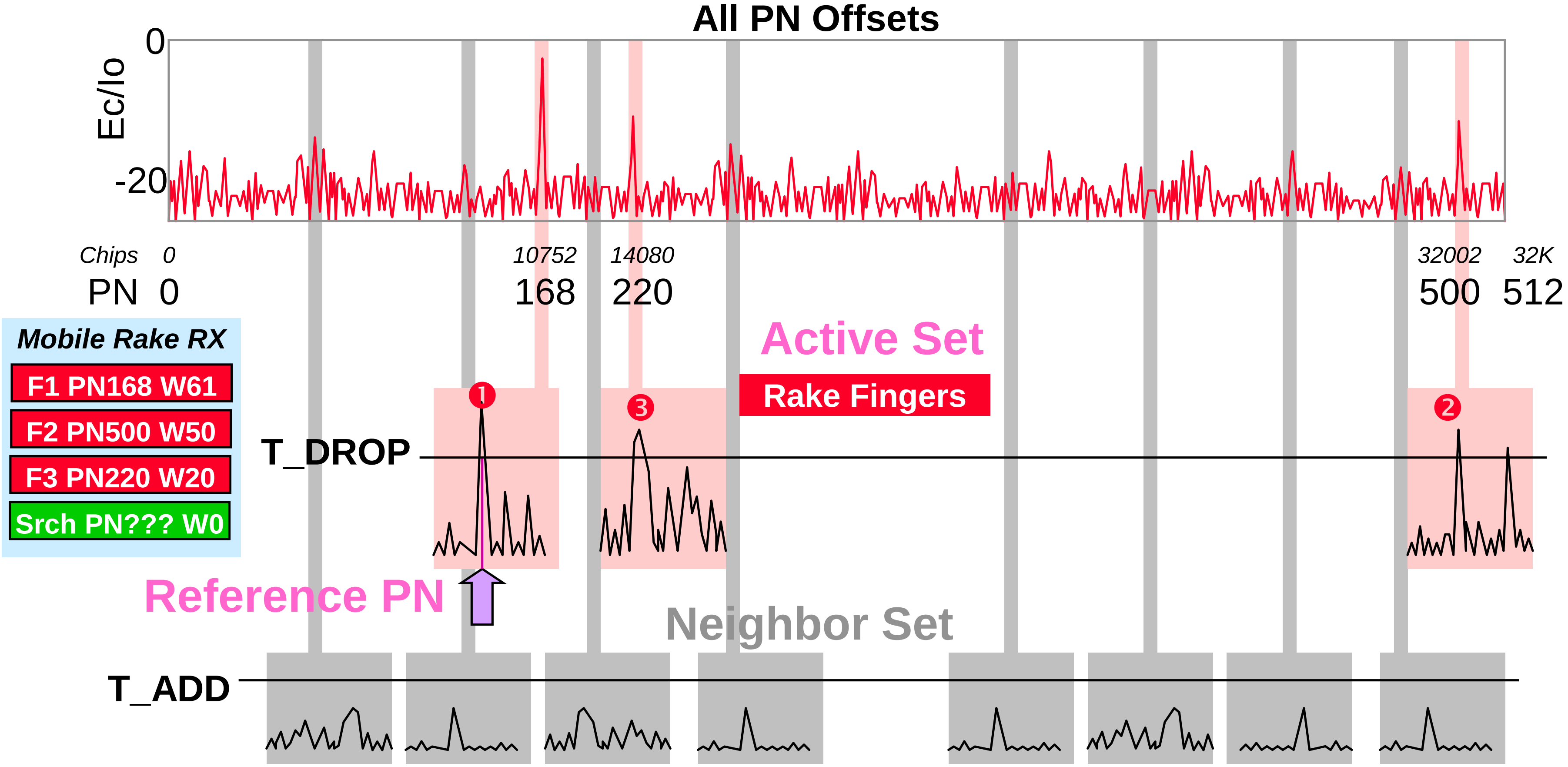
MOBILE STATION ACKNOWLEDGMENT

```
98/05/24 23:14:03.245 [RTC] Order Message
MSG_LENGTH = 56 bits  MSG_TYPE = Order Message
ACK_SEQ = 7  MSG_SEQ = 7  ACK_REQ = 0
ENCRYPTION = Encryption Mode Disabled
ORDER = Mobile Station Acknowledgement Order
ADD_RECORD_LEN = 0 bits
Order-Specific Fields = Field Omitted
RESERVED = 0
```



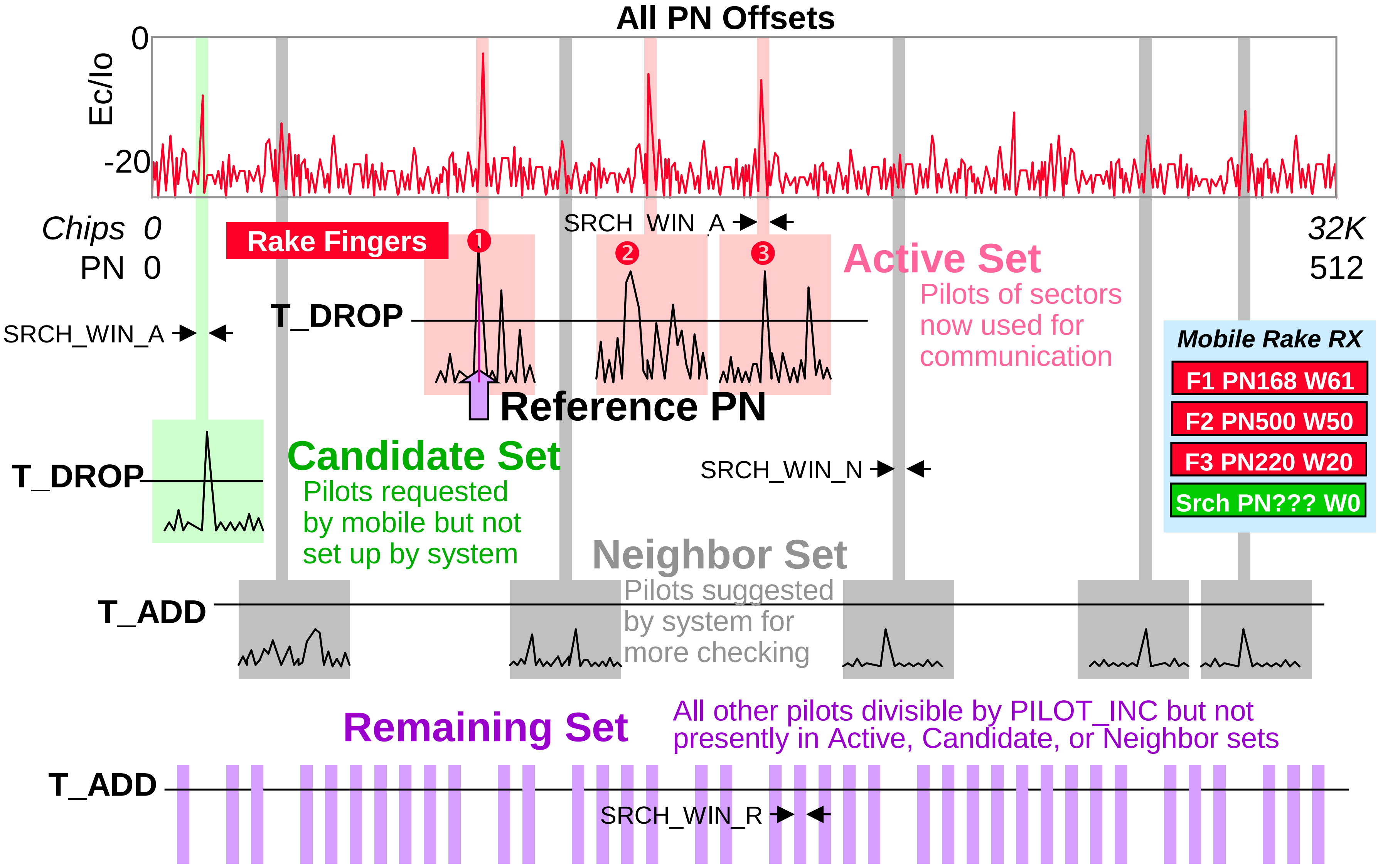
The mobile confirms receiving the Neighbor List Update Message. It is already checking the neighbor list and will do so continuously from now on. The handoff is fully established.

Handoff Now In Effect, but still check Pilots!



Continue checking each ACTIVE pilot. If any are less than T_DROP and remain so for T_TDROP time, send Pilot Strength Measurement Message, DROP IT!! Continue looking at each NEIGHBOR pilot. If any ever rises above T_ADD, send Pilot Strength Measurement Message, ADD IT!

The Complete Picture of Handoff & Pilot Sets



Active Set

Pilots of sectors now used for communication

Mobile Rake RX

- **F1 PN168 W61**
- **F2 PN500 W50**
- **F3 PN220 W20**
- **Srch PN??? W0**

Candidate Set

Pilots requested by mobile but not set up by system

Neighbor Set

Pilots suggested by system for more checking

Remaining Set

All other pilots divisible by PILOT_INC but not presently in Active, Candidate, or Neighbor sets

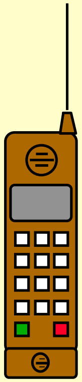
Section G

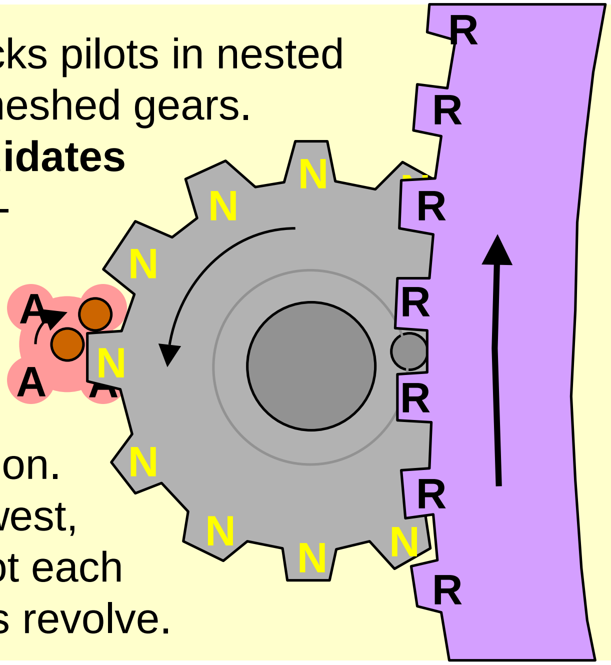
Deeper Handoff Details: Search Windows & Timing

The Pilot Searcher's Measurement Process

CURRENT PILOT SET CONTENTS

3	A	A	A									
1	C											
12	N	N	N	N	N	N	N	N	N	N	N	N
112	R	R	R	R	R	R	R	R	R	R	R	R
	R	R	R	R	R	R	R	R	R	R	R	R
	R	R	R	R	R	R	R	R	R	R	R	R
	R	R	R	R	R	R	R	R	R	R	R	R
	R	R	R	R	R	R	R	R	R	R	R	R
	R	R	R	R	R	R	R	R	R	R	R	R
	R	R	R	R	R	R	R	R	R	R	R	R
	R	R	R	R	R	R	R	R	R	R	R	R
	R	R	R	R	R	R	R	R	R	R	R	R
	R	R	R	R								





The searcher checks pilots in nested loops, much like meshed gears. **Actives and candidates** occupy the fastest-spinning wheel. **Neighbors** are next, advancing one pilot for each Act+Cand. revolution. **Remaining** is slowest, advancing one pilot each time the Neighbors revolve.

PILOT SEARCHER VIEWED IN SEQUENCE: Typical Elapsed Time = 4 seconds

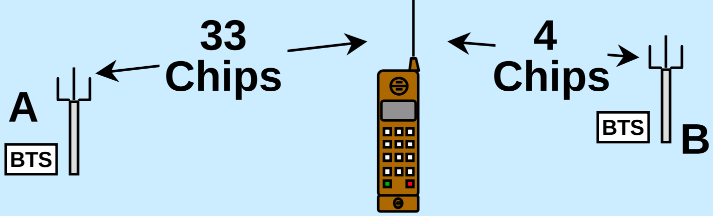
A	A	A	C	N	A	A	A	C	N	A	A	A	C	N	A	A	A	C	N	A	A	A	C	N	A	A	A	C	N	A	A	A	C	N
A	A	A	C	N	A	A	A	C	N	A	A	A	C	N	A	A	A	C	N	A	A	A	C	N	R	A	A	A	C	N	A	A	A	C
N	A	A	A	C	N	A	A	A	C	N	A	A	A	C	N	A	A	A	C	N	A	A	A	C	N	A	A	A	C	N	A	A	A	C
N	A	A	A	C	N	A	A	A	C	N	A	A	A	C	N	R	A	A	A	C	N	A	A	A	C	N	A	A	A	C	N	A	A	A
C	N	A	A	A	C	N	A	A	A	C	N	A	A	A	C	N	A	A	A	C	N	A	A	A	C	N	A	A	A	C	N	A	A	A
C	N	A	A	A	C	N	R																											

Only 3 of 112 remaining set pilots have been checked thus far!

A Quick Primer on Pilot Search Windows

- The phone chooses one strong sector and “locks” to it, accepting its offset at “face value” and interpreting all other offsets by comparison to it
- In messages, system gives to handset a neighbor list of nearby sectors’ PNs
- Propagation delay “skews” the apparent PN offsets of all other sectors, making them seem earlier or later than expected
- To overcome skew, when the phone searches for a particular pilot, it scans an extra wide “delta” of chips centered on the expected offset (called a “search window”)
- Search window values can be datafilled individually for each Pilot set:
- There are pitfalls if the window sizes are improperly set
  - too small: overlook pilots from far away
  - too large: search time increases
  - too large: might misinterpret identity of a distant BTS’ signal

PROPAGATION DELAY SKEWS APPARENT PN OFFSETS



If the phone is locked to BTS A, the signal from BTS B will seem 29 chips earlier than expected.
If the phone is locked to BTS B, the signal from BTS A will seem 29 chips later than expected.

One chip is 801 feet or 244.14 m
1 mile=6.6 chips; 1 km.= 4.1 chips

Setting Pilot Search Window Sizes

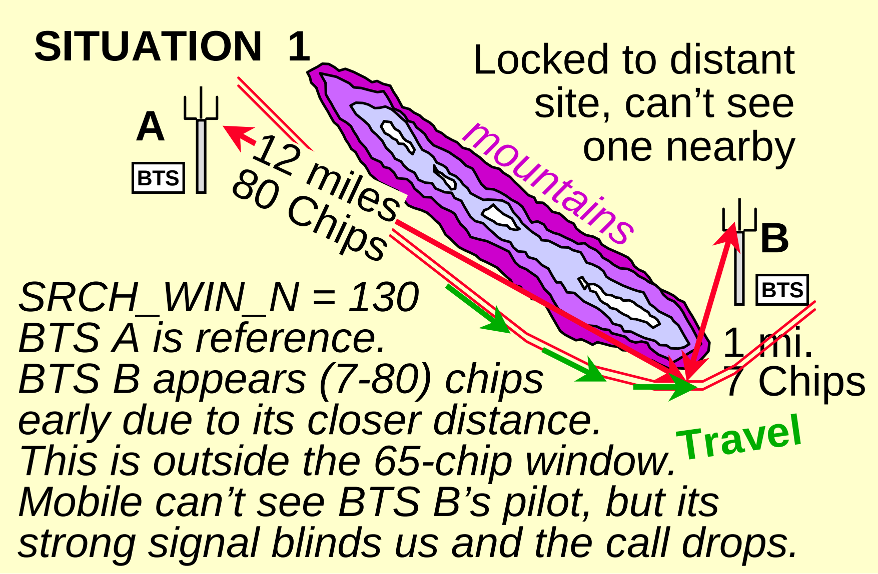
- When the handset first powers up, it does an exhaustive search for the best pilot. No windows are used in this process.
- On the paging channel, the handset learns the window sizes SRCH_WIN_A, N, R and uses them when looking for neighbors both in idle mode and during calls.
- When a strong neighbor is requested in a PSMM, the former neighbor pilot is now a candidate. Its offset is precisely remembered and frequently rechecked and tracked by the phone.
- Window size for actives and candidates can be small, since their exact position is known. Only search wide enough to include multipath energy!
  - This greatly speeds up overall searching!
- Most post-processing tools deliver statistics on the spread (in chips) between fingers locked to the same pilot. These statistics literally show us how wide the SRCH_WIN_A should be set.
- Neighbor and Remaining search windows should be set to accommodate the maximum intercell distances which a mobile might experience

SEARCH WINDOW SETTINGS AND PROPAGATION DISTANCES

Window Size (Chips)	Datafill Value	N,R Delta Distance	
		Miles	KM.
14 (±7)	4	1.06	1.71
20 (±10)	5	1.52	2.44
28 (±14)	6	2.12	3.42
40 (±20)	7	3.03	4.88
60 (±30)	8	4.55	7.32
80 (±40)	9	6.07	9.77
100 (±50)	10	7.59	12.2
130 (±65)	11	9.86	15.9
160 (±80)	12	12.1	19.5
226 (±113)	13	17.1	27.6
320 (±160)	14	24.3	39.1
452 (±226)	15	34.3	55.2

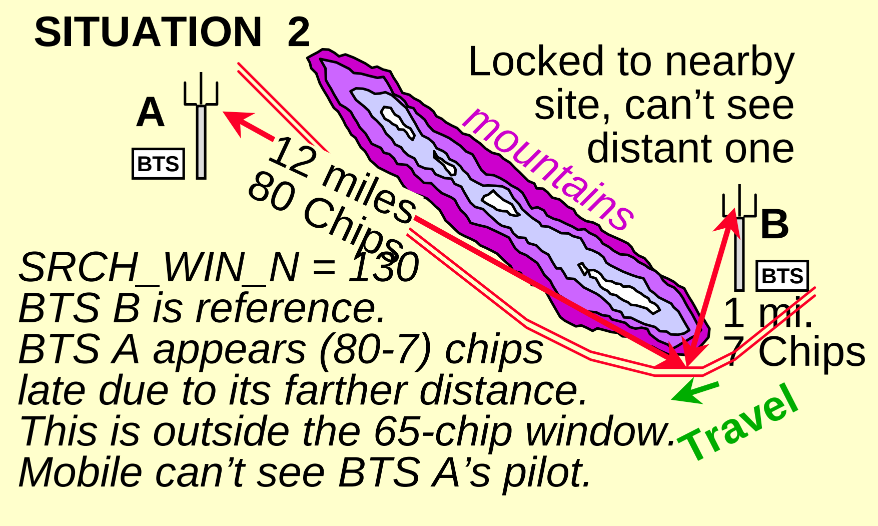
Handoff Problems: “Window” Dropped Calls

- Calls often drop when strong neighbors suddenly appear outside the neighbor search window and cannot be used to establish soft handoff.
- Neighbor Search Window SRCH_WIN_N should be set to a width at least twice the propagation delay between any site and its most distant neighbor site
- Remaining Search Window SRCH_WIN_R should be set to a width at least twice the propagation delay between any site and another site which might deliver occasional RF into the service area


SITUATION 1

Locked to distant site, can’t see one nearby

SRCH_WIN_N = 130
BTS A is reference.
BTS B appears (7-80) chips early due to its closer distance.
This is outside the 65-chip window.
Mobile can’t see BTS B’s pilot, but its strong signal blinds us and the call drops.


SITUATION 2

Locked to nearby site, can’t see distant one

SRCH_WIN_N = 130
BTS B is reference.
BTS A appears (80-7) chips late due to its farther distance.
This is outside the 65-chip window.
Mobile can’t see BTS A’s pilot.

Overall Handoff Perspective

- Soft & Softer Handoffs are preferred, but not always possible
  - a handset can receive BTS/sectors simultaneously only on *one* frequency
  - all involved BTS/sectors must connect to a *networked BSCs. Some manufacturers do not presently support this, and so are unable to do soft-handoff at boundaries between BSCs.*
  - *frame timing* must be same on all BTS/sectors
- If any of the above are not possible, handoff still can occur but can only be "hard" break-make protocol like AMPS/TDMA/GSM
  - intersystem handoff: hard
  - change-of-frequency handoff: hard
  - CDMA-to-AMPS handoff: hard, no handback
    - auxiliary trigger mechanisms available (RTD)

Section I

Introduction to Optimization

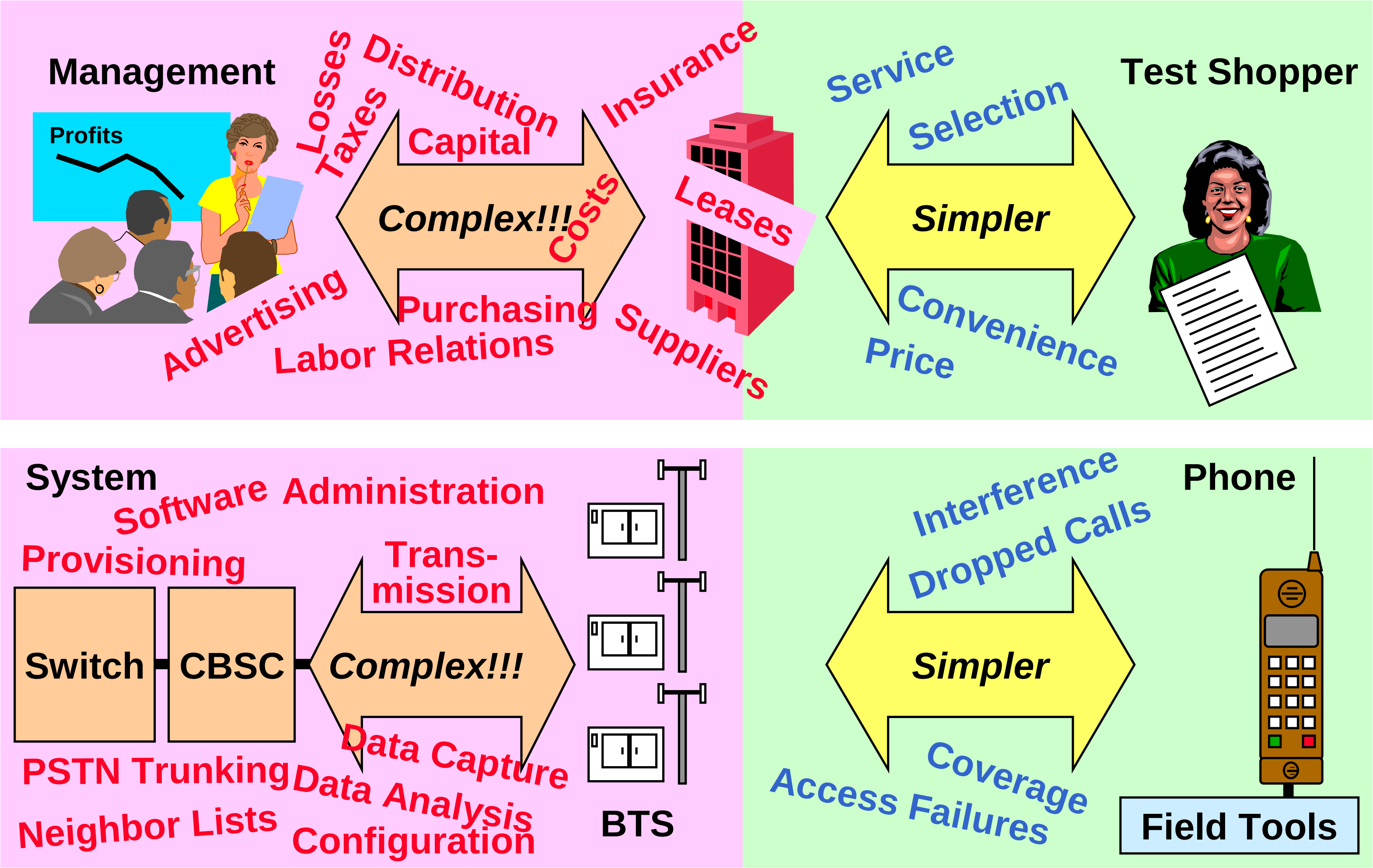
Introduction to Optimization

- Course RF200 provides detailed information on CDMA system performance optimization, and is intended for all personnel who are responsible for improving system performance. RF200 presents:
  - Performance Indicators and Problem Signatures analysis
  - Review of tools and stats available on the system
  - Review of mobile tools and how to interpret test drive data
  - How to analyze drive-test data with post-processing tools
  - Real-life examples of problems for “hands-on” analysis
- Optimization is important enough that everyone should understand what it is and how it is usually performed. The following slides provide a general perspective on optimization and are intended for everyone with technical responsibilities, even if not directly involved in performance optimization

System Performance Optimization

- The term “System Performance Optimization” really includes three distinct types of activities:
  - Optimization of a New System or New Cells
    - examining parameters, neighbor lists, and cell configuration to ensure that blatant errors are eliminated and normal operation is achieved as verified in drive tests
  - Minimization of Operating Problems on Existing Systems
    - identifying problems from system statistics, drive tests, and customer complaints
    - reducing dropped calls, access failures, trouble spots
  - Capacity Enhancement
    - watching system capacity indicators and optimizing adjustable parameters to achieve the best possible capacity, consistent with acceptable levels of dropped calls and access failures

Department Store Analogy: Tops-Down, Bottoms-Up



Management

Profits

Losses

Taxes

Distribution

Capital

Insurance

Complex!!!

Costs

Leases

Advertising

Purchasing

Labor Relations

Suppliers

Service

Selection

Test Shopper

Simpler

Convenience

Price

System

Software

Administration

Provisioning

Trans-mission

Switch

CBSC

Complex!!!

PSTN Trunking

Data Capture

Data Analysis

Neighbor Lists

Configuration

BTS

Interference

Dropped Calls

Phone

Simpler

Coverage

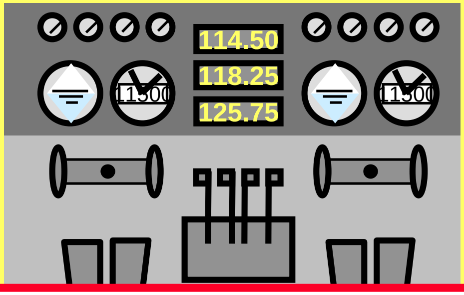
Access Failures

Field Tools

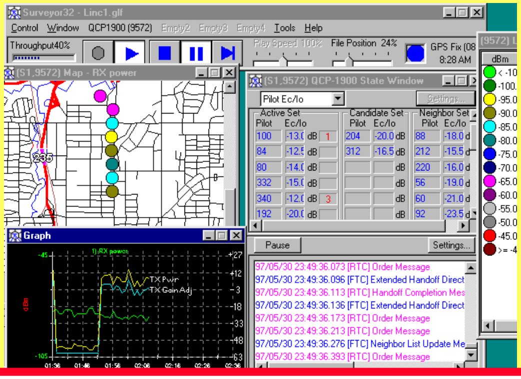
Some things are easier to measure from the customer side!

Aeronautical Analogy: Tools for Problem Investigation

Control & Parameters



Flight Data Recorder



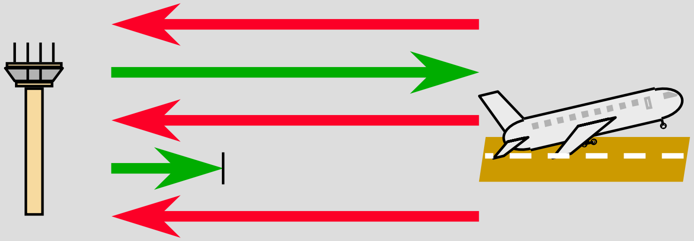
Active Set			Candidate Set		Neighbor Set	
Pilot	Ec/Io		Pilot	Ec/Io	Pilot	Ec/Io
100	-13. dB	1	204	-20.0 dB	88	-18.0 d
84	-12. dB		312	-16.5 dB	212	-15.5 d
80	-14. dB			dB	220	-16.0 d
332	-15. dB			dB	56	-19.0 d
340	-12. dB	3		dB	60	-21.0 d
192	-20. dB			dB	92	-23.5 d

```
97/05/30 23:49:36.073 [RTC] Order Message
97/05/30 23:49:36.096 [FTC] Extended Handoff Direct
97/05/30 23:49:36.113 [RTC] Handoff Completion Mes
97/05/30 23:49:36.136 [FTC] Extended Handoff Direct
97/05/30 23:49:36.173 [RTC] Order Message
97/05/30 23:49:36.213 [RTC] Order Message
97/05/30 23:49:36.276 [FTC] Neighbor List Update Me
97/05/30 23:49:36.393 [RTC] Order Message
```

Temporal Analyzer Data

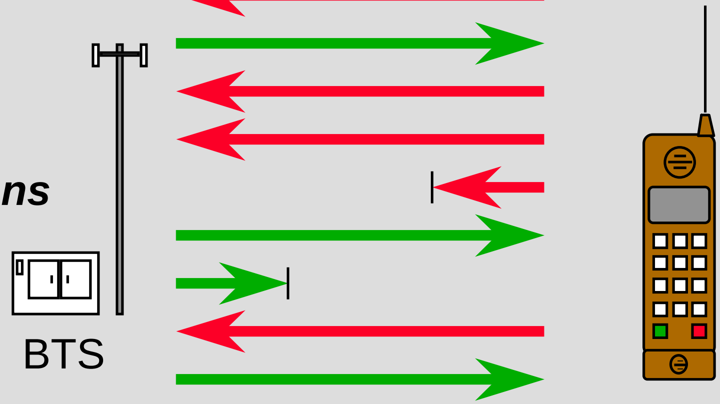
Messaging

Aeronautical Investigations



Cockpit Voice Recorder

CDMA Investigations



Layer 3 Message Files

To study the cause of an aeronautical accident, we try to recover the Flight Data Recorder and the Cockpit Voice Recorder.

To study the cause of a CDMA call processing accident, we review data from the Temporal Analyzer and the Layer 3 Message Files -- for the same reasons.

Starting Optimization on a New System

- **RF Coverage Control**
  - try to contain each sector's coverage, avoiding gross spillover into other sectors
  - tools: PN Plots, Handoff State Plots, Mobile TX plots
- **Search Window Settings**
  - find best settings for SRCH_WIN_A, _N, _R
  - especially optimize SRCH_WIN_A per sector using collected finger separation data; has major impact on pilot search speed
- **Neighbor List Tuning**
  - try to groom each sector's neighbors to only those necessary but be alert to special needs due to topography and traffic
  - tools: diagnostic data, system logs
- **Access Failures, Dropped Call Analysis**
  - finally, iterative corrections until within numerical goals

Getting these items into shape provides a solid baseline and foundation from which future performance issues can be addressed.

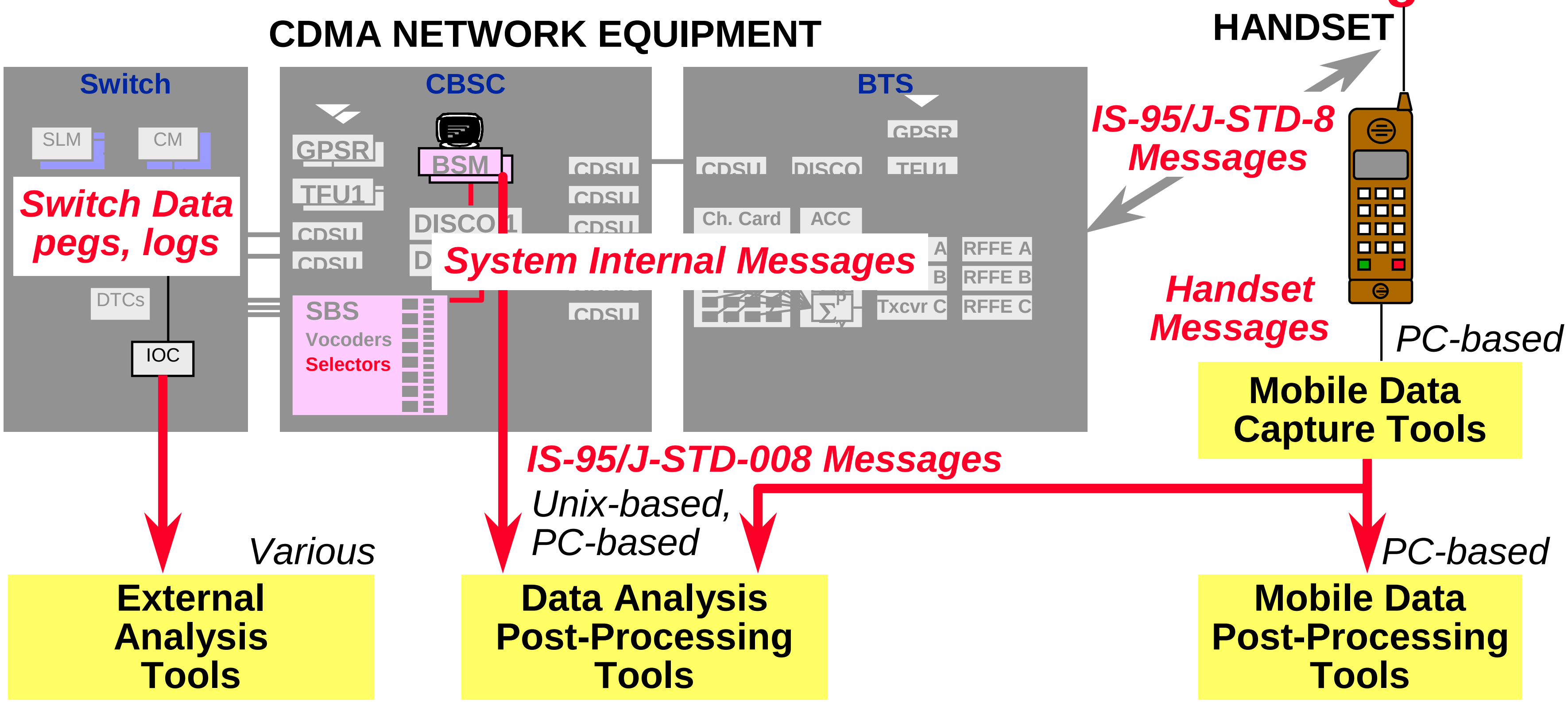
Solving Problems on Existing Systems

- CDMA optimization is very different from optimization in analog technologies such as AMPS
- AMPS: a skilled engineer with a handset or simple equipment can hear, diagnose, and correct many common problems
  - co-channel, adjacent channel, external interferences
  - dragged handoffs, frequency plan problems
- CDMA impairments have ***one audible symptom: Dropped Call***
  - voice quality remains excellent with perhaps just a hint of garbling even as the call approaches dropping in a hostile RF environment
- Successful CDMA Optimization requires:
  - recognition and understanding of common reasons for call failure
  - capture of RF and digital parameters of the call prior to drop
  - analysis of call flow, checking messages on both forward and reverse links to establish “what happened”, where, and why

CDMA Problems Attacked in Optimization

- **Excessive Access Failures**
  - typical objectives: <2% (IS-95B will bring improvements)
- **Excessive Dropped Calls**
  - typical objective: ~1%, <2%
- **Forward Link Interference**
  - typical objective: eliminate situations which prevent handoff!
- **Slow Handoff**
  - typical objective: eliminate situations which delay handoff!
- **Handoff Pilot Search Window Issues**
  - avoid handoff drops!
- **Excessive Soft Handoff**
  - control coverage, not T_Add/T_Drop, to manage soft handoff levels (~<50%)
- **Grooming Neighbor Lists**
  - “if you need it, use it!”
- **Software Bugs, Protocol Violations**
  - Neither system software, nor mobile software, nor the CDMA standard is perfect. Don’t humbly accept problems -- dig in and find out what’s happening!

Sources of CDMA Data and Tools for Processing



- CDMA optimization data flows from three places:
  - Switch
  - CDMA peripherals (CBSC & BTS)
  - Handset
- Each stream of data has a family of software and hardware tools for collection and analysis

CDMA Field Test Tools

Field Collection Tools using Handset Data

Motorola
Qualcomm
Grayson
Hewlett-Packard
SAFCO
Comarco
LCC

PN Scanners

Hewlett-Packard
Berkeley Varitronics
Grayson
Qualcomm

- There are many commercial CDMA field test tools
- Characteristics of many test tools:
  - capture data from data ports on commercial handsets
  - log data onto PCs using proprietary software
  - can display call parameters, messaging, graphs, and maps
  - store data in formats readable for post-processing analysis
  - small and portable, easy to use in vehicles or even on foot
- A few considerations when selecting test tools:
  - does it allow integration of network and mobile data?
  - Cost, features, convenience, availability, and support
  - new tools are introduced every few months - investigate!

Qualcomm’s MDM: Mobile Diagnostic Monitor

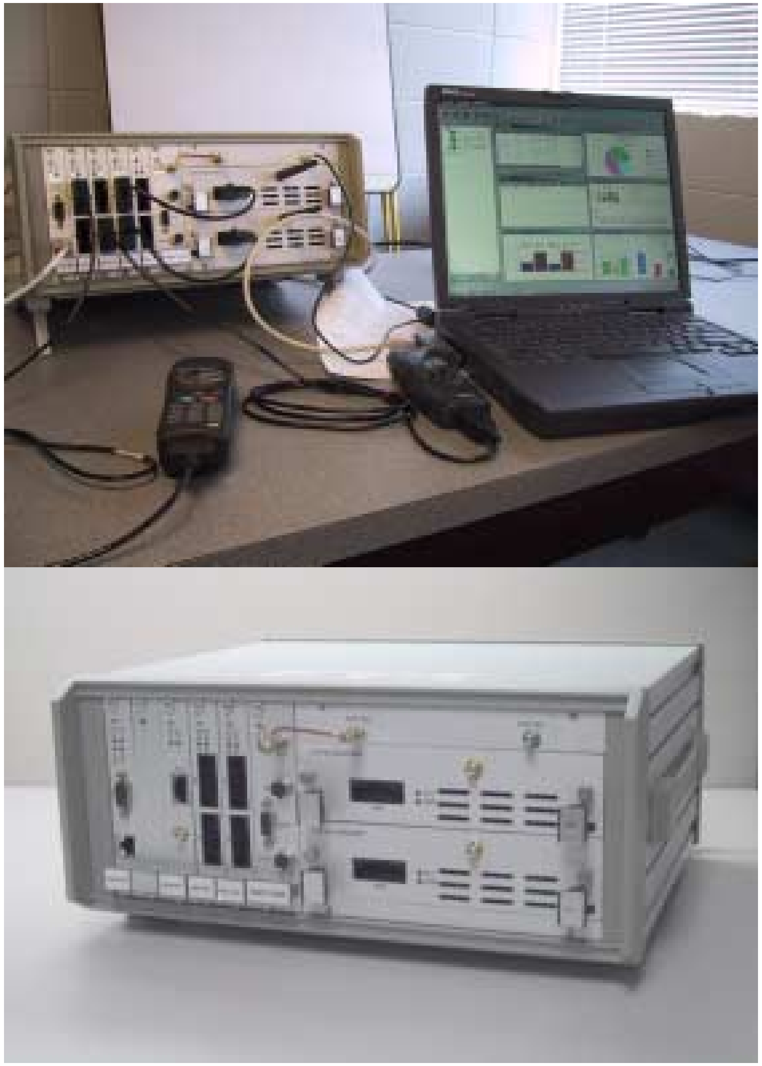
- Qualcomm’s Mobile Diagnostic Monitor
  - CDMA handset (customer provided)
  - Proprietary connecting cable
  - PC software for collection and field pre-analysis
    - Temporal analyzer display mode
    - Messaging

Grayson Electronics Mobile Collection Tools

- Wireless Measurement Instrument
  - Grayson's original hardware platform, can contain up to 4 receivers, handsets, scanners, and other devices
- Inspector32 PC collection software
  - numerous output formats & exporting - ASCII messages, database, temporal data
  - simultaneous display of parameters, map location, messaging, PN scanner
- Interpreter^{TM} post-processing software
  - call event statistics, parameters, performance indicators as map icons, graphs, and spreadsheet tables
  - message display window synched with maps and graphs
  - can search for events, messages
  - can study multiple drive files at once

Grayson’s new Invex3G Tool

- In 1Q2001 Grayson introduced its new Invex3G tool, with new features
    - 100 MB ethernet connection to PC
    - the eight card slots can hold receivers or dual-phone cards
    - there’s also room for two internal PN scanners
    - Multiple Invex units can be cascaded for multi-phone load-test applications
    - Cards are field-swappable - Users can reconfigure the unit in the field for different tasks without factory assistance



Agilent Drive-Test Tools

- Agilent offers Drive-Test tools
  - Serial interfaces for up to four CDMA phones
  - A very flexible digital receiver with several modes
- PN Scanner
  - Fast, GPS-locked, can scan two carrier frequencies
- Spectrum Analyzer
  - Can scan entire 800 or 1900 mHz. Bands
- Base-Station Over-Air Tester (BOAT)
  - Can display all walsh channel activity on a specific sector
  - Useful for identifying hardware problems, monitoring instantaneous traffic levels, etc.
- Post-Processing tool: OPAS32

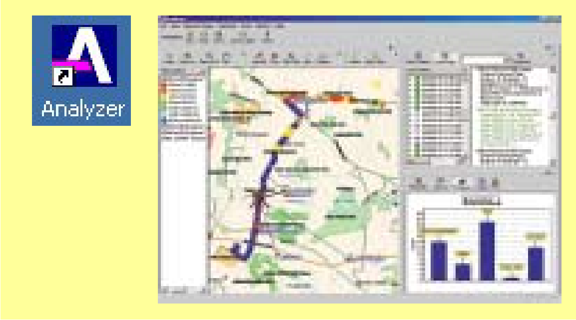
Comarco Mobile Tools

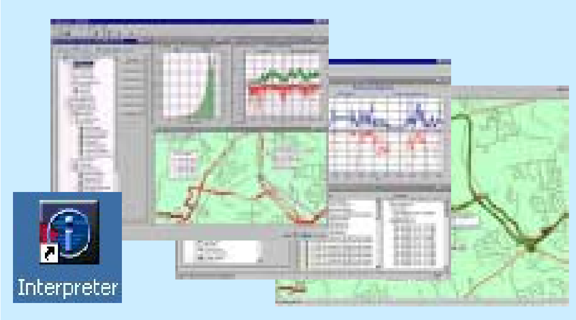
- X-Series Units for more data-intensive collection activities
  - Multiple handsets can be collected
  - Data is displayed and collected on PC
- LT-Series provides integrated display and logging
- "Workbench" Post-Processing tool analyzes drive-test files

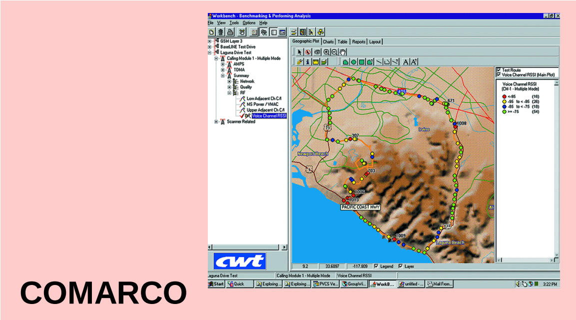
Post-Processing Tools

Post-Processing tools display drive-test files for detailed analysis - Faster, more effective than studying data playback with collection tools alone

- Actix Analyzer
  - Imports/analyzes data from almost every brand of drive-test collection tool
- Grayson Interpreter
  - Imports/analyzes data from Grayson Wireless Inspector, Illuminator, and Invex3G
- Agilent OPAS32
  - Imports/analyzes a variety of data
- Nortel RF Optimizer
  - Can merge/analyze drive-test and Nortel CDMA system data
- Wavelink
- Comarco "Workbench" Tool
- Verizon/Airtouch internal tool







PN Scanners

- PN Scanners are faster than phones and more reliable finding rogue pilots
- **Berkeley Varitronics** (GPS-referenced)
  - full-PN scan speed 26-2/3 ms.
  - 2048 parallel processors for very fast detection of transient interferors
- **Hewlett-Packard** (GPS-referenced)
  - full-PN scan speed 1.2 sec.
  - Integrated with spectrum analyzer and phone call-processing tool
- **Qualcomm** (BTS-referenced)
  - lowest-cost solution
  - also acts as test phone with user-set T_Add, T_Drop, etc.
- **Grayson Wireless** (BTS-referenced)
  - scan speed 6.3 sec.
  - integrated with phone & call-processing data collection tool
  - a high-end version is also available using Berkeley Scanner (GPS-locked)

Drive-Tests: Phones

Maintenance Features of CDMA Handsets

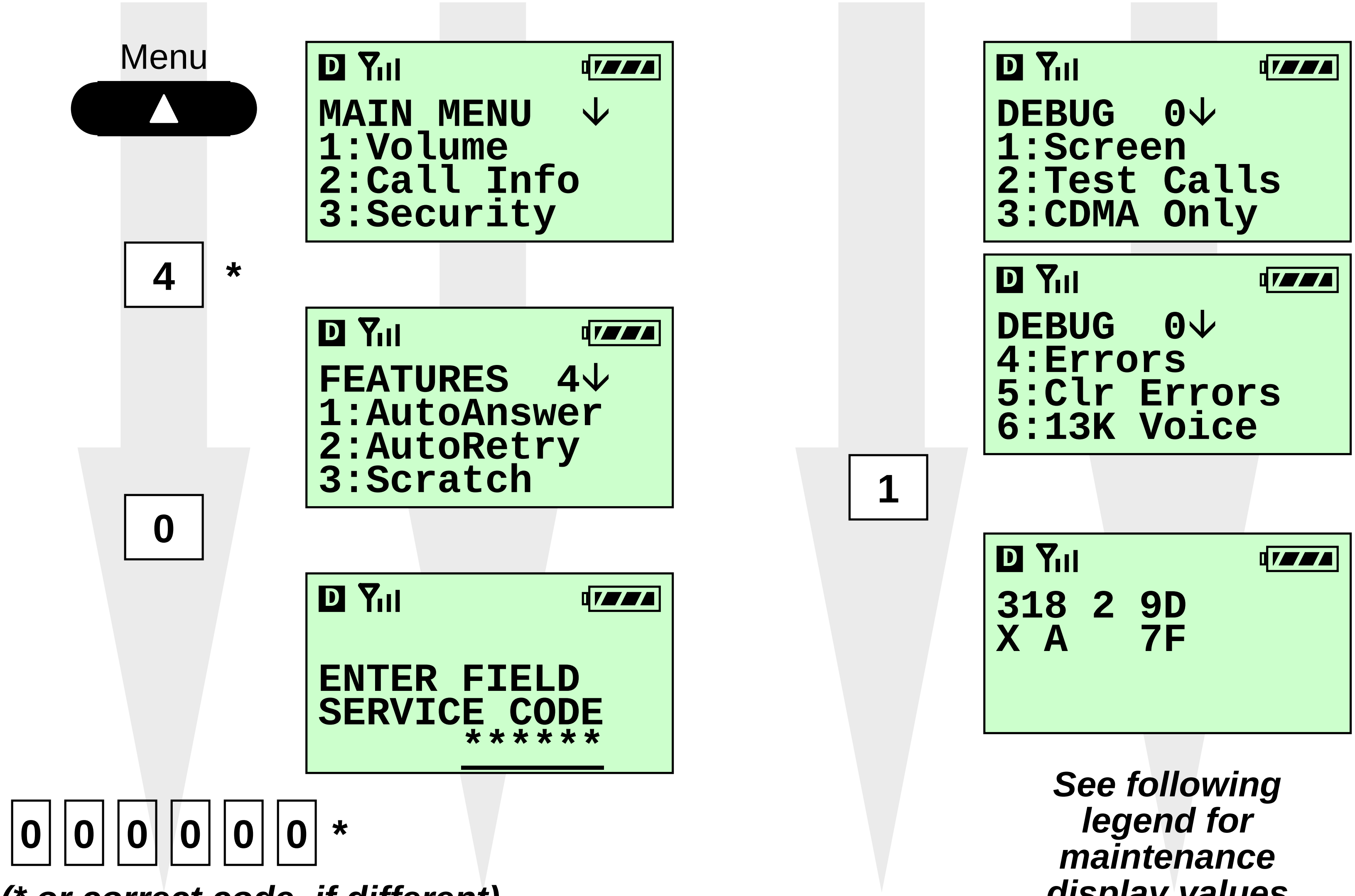
Handsets as Tools: Simple but always Available!

- Most CDMA handsets provide some form of maintenance display (“Debug Mode”) as well as instrumentation access
  - all CDMA drive-test tools use handsets as their “front-ends”

Using the handset as a manual tool without Commercial Test Tools:

- Enter the maintenance mode by special sequence of keystrokes
- Displayed Parameters
  - PN Offset, Handset Mode, Received RF Level , Transmit Gain Adjust
- Maintenance Display Applications
  - best serving cell/sector
  - simple call debugging (symptoms of weak RF, forward link interference, etc.)
- Handset Limitations during manual observation
  - no memory: real-time observations only; no access to messages or call details; serving PN offset not updated during voice calls

Older Qualcomm/Sony Maintenance Displays



Press This: *See This:* *continue:* *See This:*

```
D
MAIN MENU   ↓
1:Volume
2:Call Info
3:Security
```

4 *

```
D
FEATURES  4↓
1:AutoAnswer
2:AutoRetry
3:Scratch
```

0

```
D

ENTER FIELD
SERVICE CODE
      ******
```

0 0 0 0 0 0 *

(or correct code, if different)*

1

```
D
DEBUG  0↓
1:Screen
2:Test Calls
3:CDMA Only
```

```
D
DEBUG  0↓
4:Errors
5:Clr Errors
6:13K Voice
```

```
D
318 2 9D
X A   7F
```

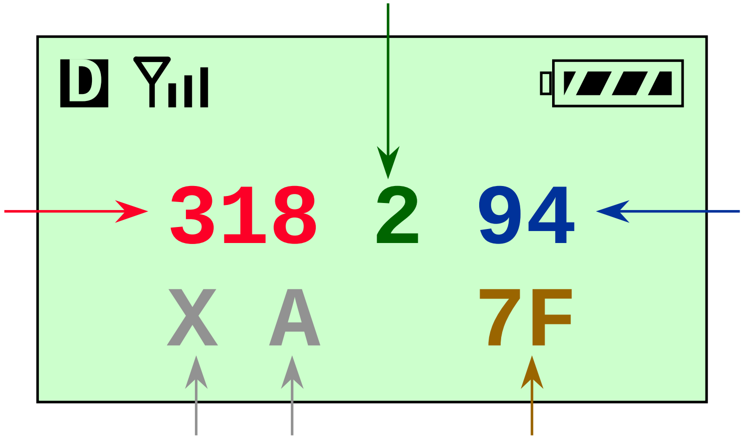
See following legend for maintenance display values

Qualcomm & Sony Phones with Jog Dials

- Enter 111111
- Press dial in for OPTIONS
- Dial to FIELD DEBUG, press
- enter Field Debug Security Code
- press Screen

Interpreting the QCP Maintenance Display

0 - Pilot Channel Acquisition Substate
1 - Sync Channel Acquisition Substate
2 - MS Idle State
3 - System Access State
4 - Traffic Channel State



Receive State

PN Offset

Receive Power

Unsupported
A = active pilots
X = exit reason

Transmit Adjust

80	-109
80	-109
00	0
0A	-5
14	-10
1E	-15
28	-20

	QCP-1900	QCP-800
FF	-67	-64
F5	-70	-67
E6	-75	-72
D7	-80	-77
C8	-85	-82
B9	-90	-87
AA	-95	-92
9B	-100	-97
8C	-105	-102
80	-109	-106

Receive Power Conversion:

$RX_{dbm}=XX_{DEC} / 3 - 63.25$ (800 MHz)

$RX_{dbm}=XX_{DEC} / 3 - 66.25$ (1900 MHz)

(if XX>7F, use $XX = XX_{DEC}-256$*)*

Transmit Gain Adjust Conversion:

$TXADJ_{db}=XX_{DEC} / 2$

Transmit Power Output Conversion:

$TX_{dbm}= -73 -RX_{DBM} - TXADJ_{db}$ (800 MHz)

$TX_{dbm}= -76 -RX_{DBM} - TXADJ_{db}$ (1900 MHz)

Kyocera 2035 Maintenance Mode

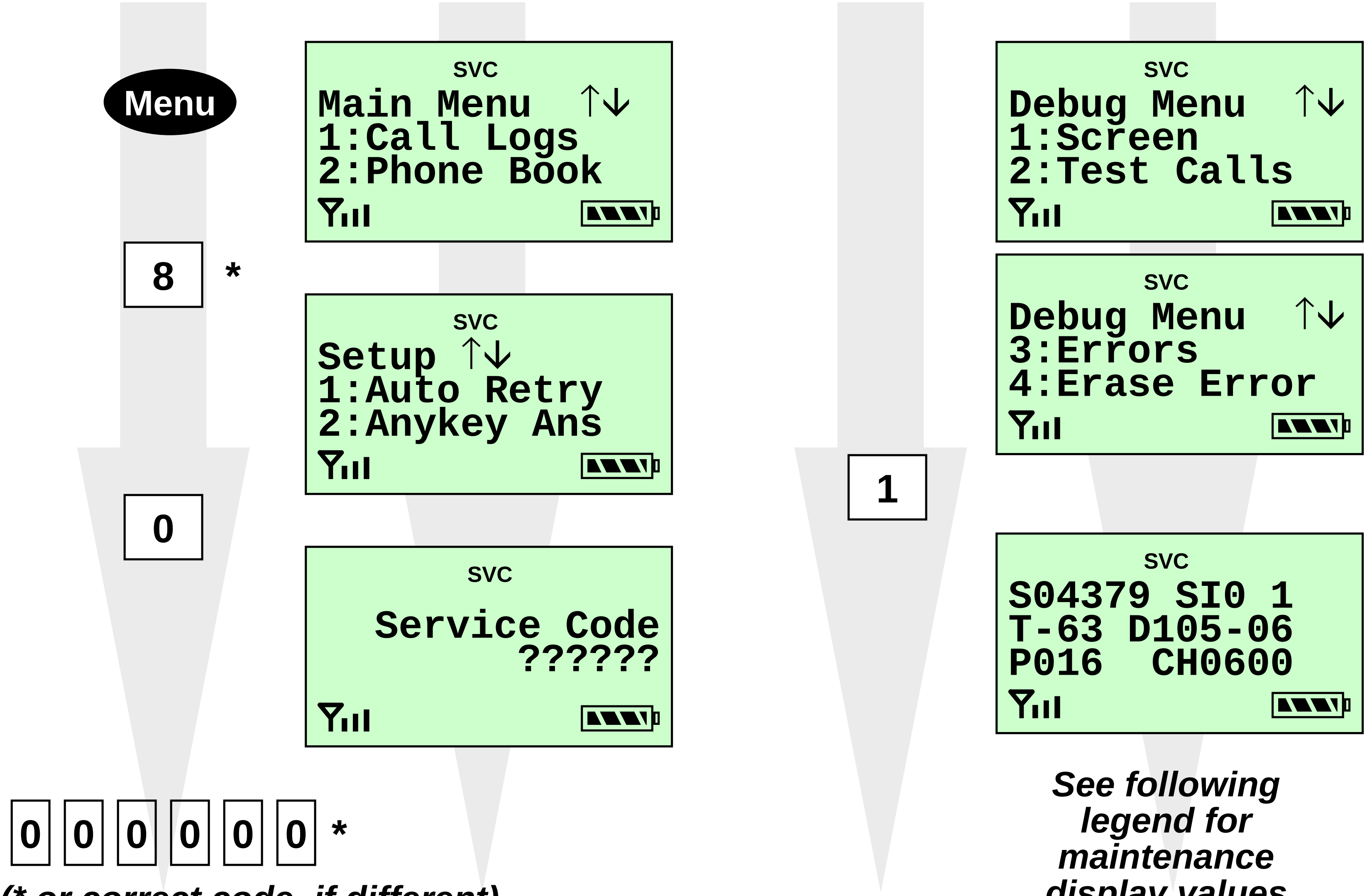
Steps to enter maintenance mode:

- 111111
- Enter
- Options: Debug
- Enter
- Enter Field Debug Code
  - 000000
- Field Debug
- Debug Screen
- Enter
- Basic
- Enter

Kyocera 6035 Maintenance Mode

- 111111
- Jog > Options
- Jog > Debug
- Open flip to continue
- Enter Code
    - 0 0 0 0 0 0
- OK
- SCREEN

Early Samsung Maintenance Display



Press This: | **See This:** | **continue:** | **See This:**

Menu

```
         SVC
Main Menu   ↑↓
1:Call Logs
2:Phone Book
```

8 *

```
         SVC
Setup ↑↓
1:Auto Retry
2:Anykey Ans
```

0

```
         SVC
    Service Code
          ??????
```

0 0 0 0 0 0 *

(or correct code, if different)*

```
         SVC
Debug Menu  ↑↓
1:Screen
2:Test Calls
```

```
         SVC
Debug Menu  ↑↓
3:Errors
4:Erase Error
```

1

```
         SVC
S04379 SI0 1
T-63 D105-06
P016  CH0600
```

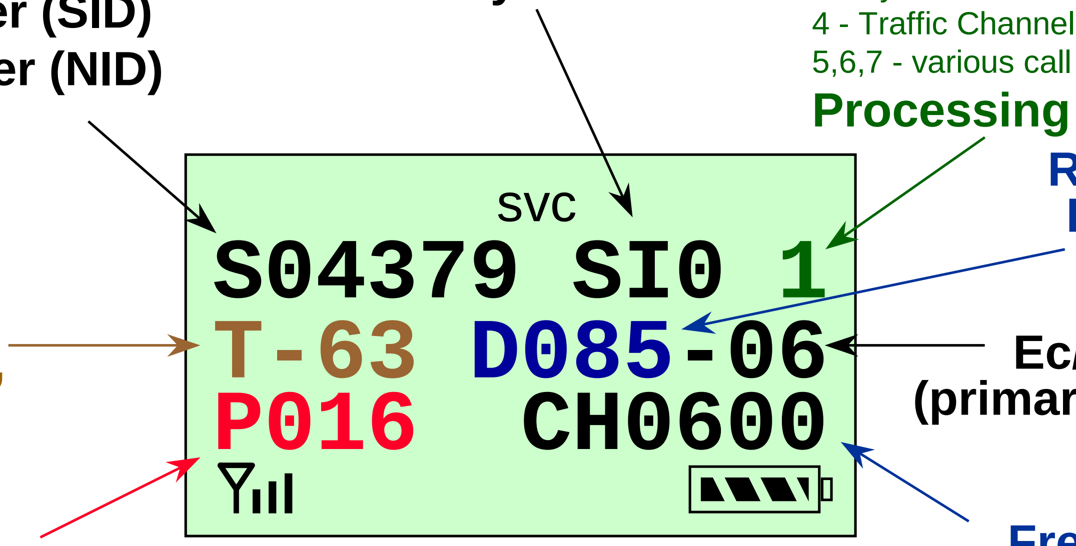
See following legend for maintenance display values

Samsung SCH-3500 Maintenance Display

Here are the steps to enter maintenance mode:

- MENU
- SETUP
- 0 (undocumented "trap door")
- 000000 (operator's code)
- Screen

Interpreting Samsung Maintenance Display: Acquisition, Idle, and Access States



Display toggles between:
System Identifier (SID)
Network Identifier (NID)

Slot Cycle Index

0 - Pilot Channel Acquisition Substate
1 - Sync Channel Acquisition Substate
2 - MS Idle State
3 - System Access State
4 - Traffic Channel State
5,6,7 - various call service options

Processing State

Receive Power, dbm

Transmit Gain Adjust, db

Ec/Io, db (primary PN only)

PN Offset

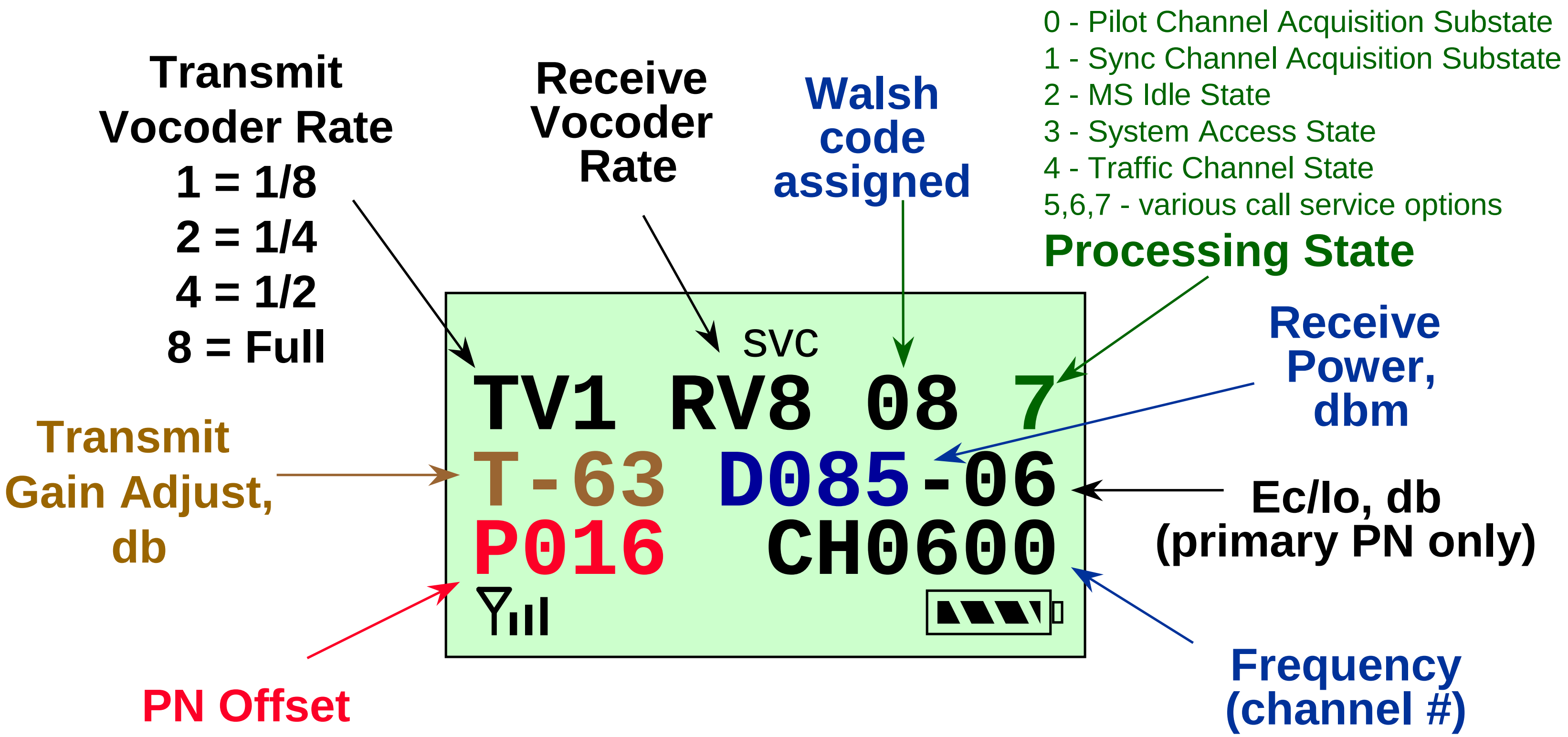
Frequency (channel #)

Transmit Power Output Calculation:

$TX_{dbm}= -73 -RX_{DBM} - TXADJ_{db}$ (800 MHz)

$TX_{dbm}= -76 -RX_{DBM} - TXADJ_{db}$ (1900 MHz)

Interpreting Samsung Maintenance Display: Traffic Channel State



Transmit Vocoder Rate
1 = 1/8
2 = 1/4
4 = 1/2
8 = Full

Receive Vocoder Rate

Walsh code assigned

0 - Pilot Channel Acquisition Substate
1 - Sync Channel Acquisition Substate
2 - MS Idle State
3 - System Access State
4 - Traffic Channel State
5,6,7 - various call service options

Processing State

Receive Power, dbm

Transmit Gain Adjust, db

Ec/Io, db (primary PN only)

PN Offset

Frequency (channel #)

Transmit Power Output Calculation:

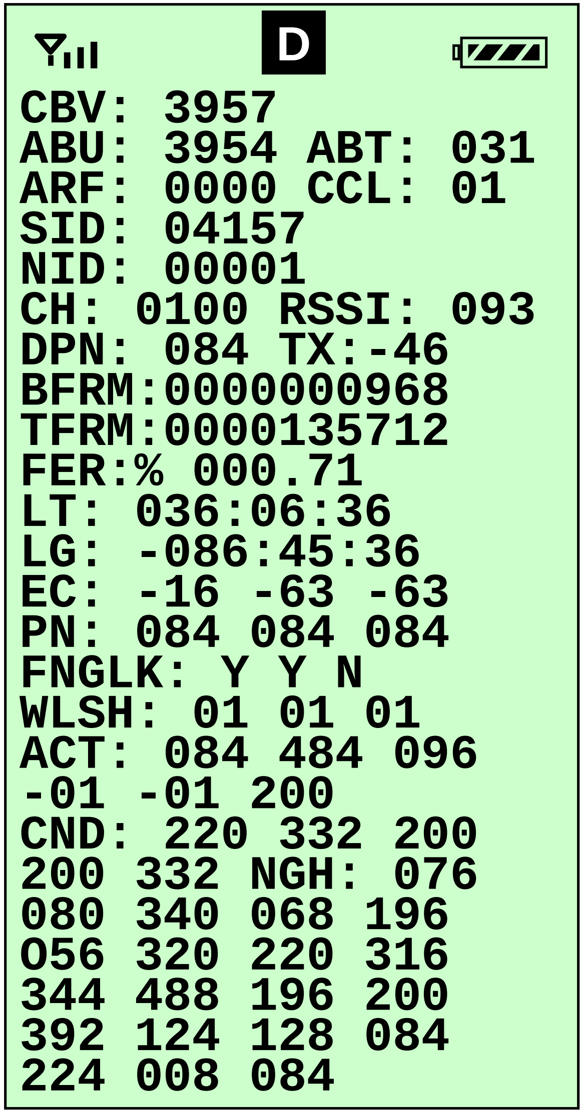
TX_{dbm}= -73 -RX_{DBM} - $TXADJ_{db}$ (800 MHz)

TX_{dbm}= -76 -RX_{DBM} - $TXADJ_{db}$ (1900 MHz)

Entering Denso Debug Mode

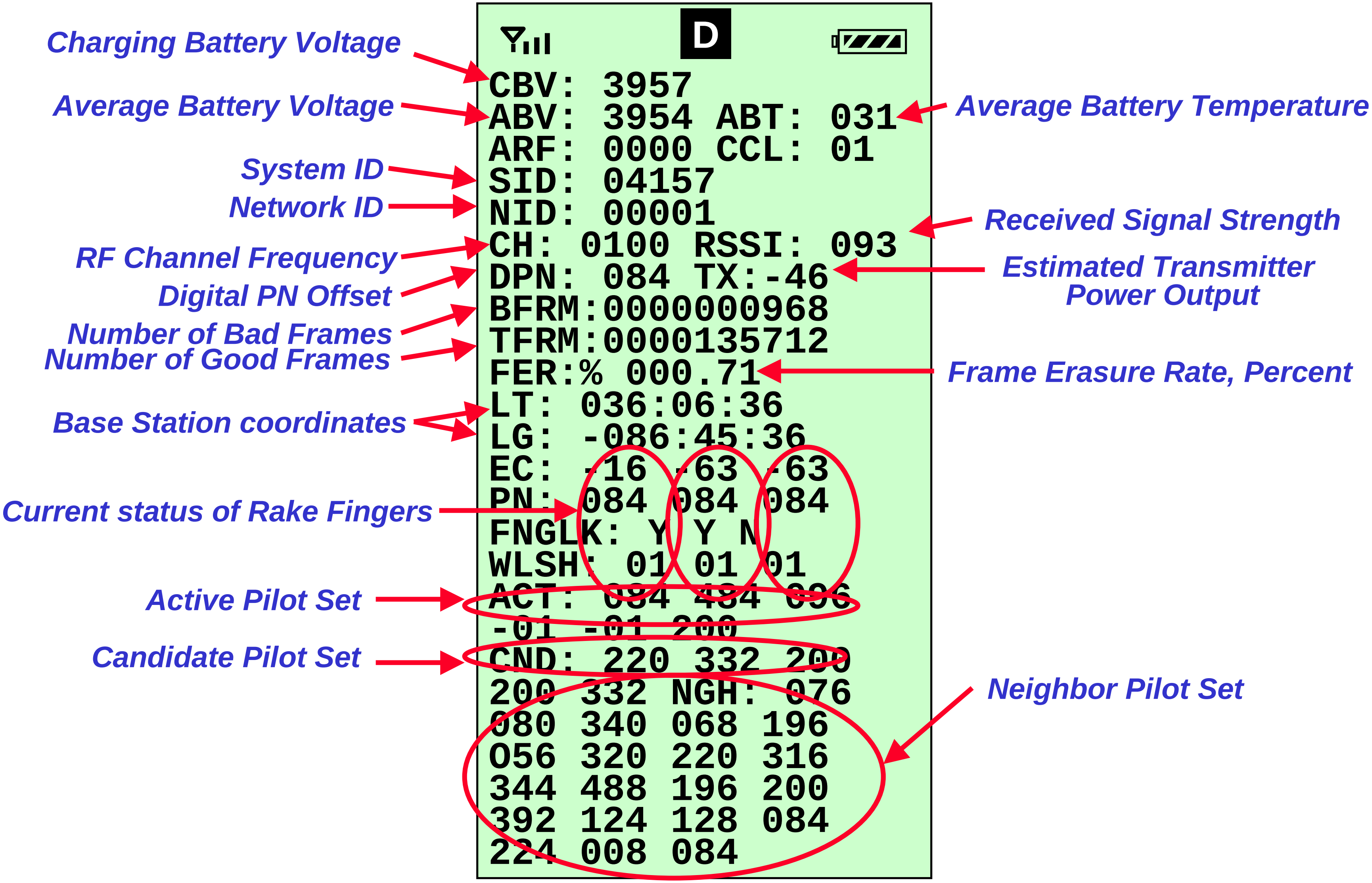
- Enter ##DEBUG (##33284)
- Scroll down to SAVE
- Press OK
- Highlight SERVICE SCREEN
- Press OK

- If you want to make a test call, dial the digits and press OK while in idle mode



```
CBV: 3957
ABU: 3954 ABT: 031
ARF: 0000 CCL: 01
SID: 04157
NID: 00001
CH: 0100 RSSI: 093
DPN: 084 TX:-46
BFRM:000000968
TFRM:000135712
FER:% 000.71
LT: 036:06:36
LG: -086:45:36
EC: -16 -63 -63
PN: 084 084 084
FNGLK: Y Y N
WLSH: 01 01 01
ACT: 084 484 096
-01 -01 200
CND: 220 332 200
200 332 NGH: 076
080 340 068 196
056 320 220 316
344 488 196 200
392 124 128 084
224 008 084
```

Denso Maintenance Display



```
D
CBV: 3957
ABV: 3954 ABT: 031
ARF: 0000 CCL: 01
SID: 04157
NID: 00001
CH: 0100 RSSI: 093
DPN: 084 TX:-46
BFRM:0000000968
TFRM:0000135712
FER:% 000.71
LT: 036:06:36
LG: -086:45:36
EC: -16 -63 -63
PN: 084 084 084
FNGLK: Y Y N
WLSH: 01 01 01
ACT: 084 484 096
-01 -01 200
CND: 220 332 200
200 332 NGH: 076
080 340 068 196
056 320 220 316
344 488 196 200
392 124 128 084
224 008 084
```

Charging Battery Voltage

Average Battery Voltage

System ID

Network ID

RF Channel Frequency

Digital PN Offset

Number of Bad Frames

Number of Good Frames

Base Station coordinates

Current status of Rake Fingers

Active Pilot Set

Candidate Pilot Set

Average Battery Temperature

Received Signal Strength

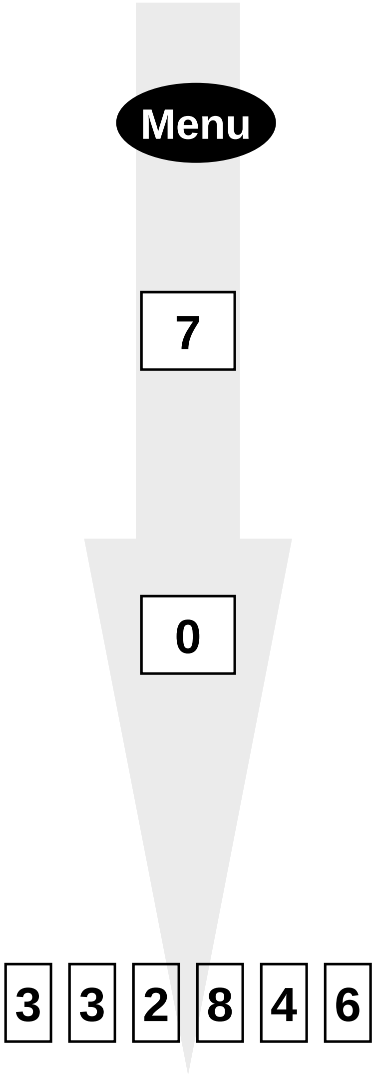
Estimated Transmitter Power Output

Frame Erasure Rate, Percent

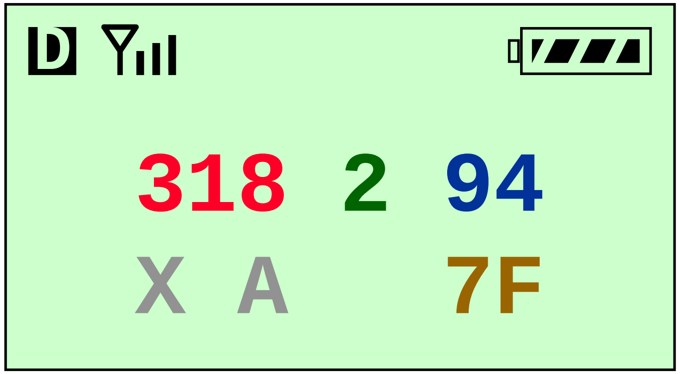
Neighbor Pilot Set

Early Sanyo Dual-Band Phones

Press This:



- press menu 7, 0
- enter in DEBUGM (332846)
- screens are similar to QCP phones



Sanyo SPC-4500 Maintenance Display

- Choose the following:
- DISPLAY
- OK
- 0
- OK
- Enter Code: 0 0 0 0 0 0
- Debug Menu
- SCREEN
- OK

Entering Maintenance Mode: Motorola

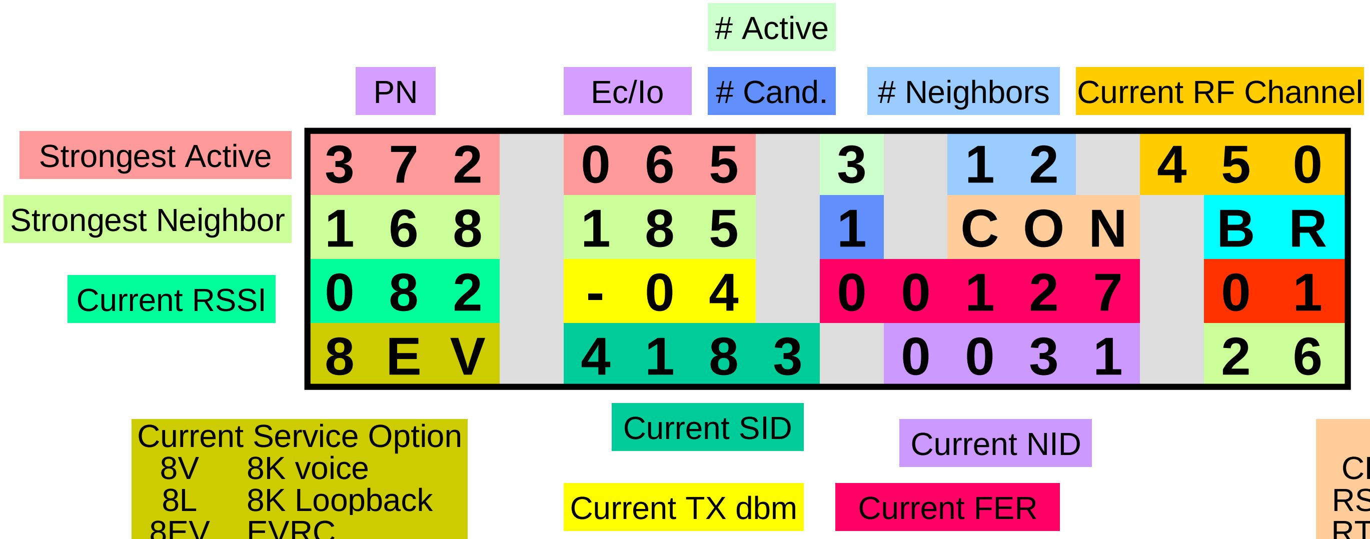
Contact your service provider to obtain your phone’s Master Subscriber entity Lock (MSL). Then enter the following:

- FCN 000000 000000 0 RCL You'll be prompted for your MSL, enter it and press STO.
  - New prompts will appear, Press STO in response to each prompt until no more appear. Don’t delay - continue quickly and enter:
- FCN 0 0 * * T E S T M O D E STO
  - The display will briefly show US then just '.
- Press 55#.
  - Step 1 will appear with its current setting displayed. Press * to accept and move on to the next step. Repeat for steps 2-8.
- Step 9 (Option byte 2) is the only step requiring manual changes. Enter 1 0 0 0 0 0 0 0 (The leftmost bit now set to '1' is what enables test mode.)
- Now press STO to accept the entry and exit back to the ' prompt.
- Power off and back on.
- You should now be in test mode!

Motorola Maintenance Display

Last Call Indicator

NI	No Indication
MR	Mobile Release
BR	Base Release
TC	Traffic Channel Lost
L2	Layer 2 Ack Fail
NC	No Channel Asn Msg
N5	N5M failure
BS	BS Ack Failure
WO	L3 WFO State Timeout
MP	Max Probe Failure
PC	Paging Channel Loss
RR	Reorder or Rel on PCH
??	Unknown Condition



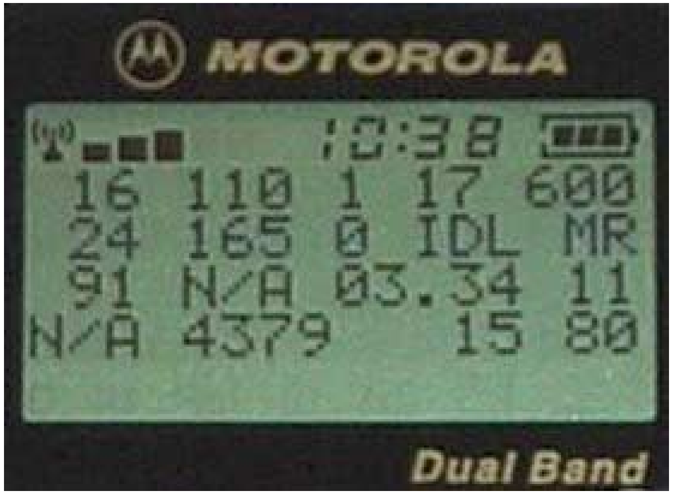
3	7	2		0	6	5		3		1	2		4	5	0
1	6	8		1	8	5		1		C	O	N		B	R
0	8	2		-	0	4		0	0	1	2	7		0	1
8	E	V		4	1	8	3		0	0	3	1		2	6

Dropped Call Counter

Call Counter

Current Service Option

8V	8K voice
8L	8K Loopback
8EV	EVRC
8S	8K SMS
13L	13K Loopback
13S	13K SMS
8MO	8K Markov Old
DAT	Data
8M	8K Markov
13M	13K Markov
13v	13K Voice
N/A	Null



```
10:38
16  110  1  17  600
24  165  0  IDL  MR
91  N/A  03.34  11
N/A 4379     15  80
```

Call Processing State

CP	CP Exit
RST	CP Restart
RTC	Restricted
PLT	Pilot Acquire
SYN	Synch Acquire
TIM	Timing
BKS	Background Search
IDL	Idle
OVD	Overhead
PAG	Paging
ORG	Call Origination
SMS	SMS
ORD	Order Response
REG	Registration
TCI	Traffic Channel Init
WFO	Waiting for Order
WFA	Waiting for Answer
CON	Conversation
REL	Release
NON	No State

NeoPoint Phones

- Although NeoPoint went out of business in June, 2001, there are still many NeoPoint handsets in general use
- Press the M (menu) key
- Select Preferences (using the up-arrow key)
- Enter 040793
- Choose Debug Screen [Select]
- Now you're in maintenance mode!

GoldStar TouchPoint

- To enter maintenance mode, just key in:

D E B U G SAVE

```
CP State:IDLE
SCI:2
SID:04139
NID:00041
CH #:0050
ACT:053
```

```
NGH:492 496 008
120 412 084 388
Rx.Eo/Io:-085
Tx.Adjust:-63
FER:% 000.02
Batt:3.82
```

Nokia 6185 Maintenance Display

- Enter *3001#12345# MENU
- Scroll down to Field test
- Press Select
- Scroll up to Enabled
- Press OK
- Power the phone off and on
- You should now be in Field test mode

```
IDLE 0050 SP
304   11    1H
00C 431 00 0
-073-075
Menu     Names
```

Older Nokia Models Maintenance Display

- Enter *3001#12345# MENU
- Scroll down to Field test
- Press Select
- Scroll up to Enabled
- Press OK
- Power the phone off and on
- You should now be in Field test mode and the following screens will be available:

Maintenance Display Screens of Nokia Handsets

The following screens appear in field test mode on Nokia HD881 series of Handsets:

Screen 1: General	
CSST	CS State
XXXXX	Idle: PN Offset TFC: #Actv, FER
RSSI	RSSI dBm
CCCC	Paging Channel #
RX	RX power, dbm
TX	TX power, dbm

Screen 2: Paging CH Info	
CSST	CS State
PGCH	Paging Channel #
CURSO	Current Service Option
FER	Frame Error Rate

Screen 4: NAM Info	
OwnNumber	Mobile MIN
ESN	Mobile Station ESN
P	Preferred Sys 1=AMPS, 2=CDMA
A	Operator Selected (1=A, 2=B, 3=both

Screen 5: NAM Info	
PPCA	Primary Channel A
SPCA	Secondary Channel A
PPCB	Primary Channel B
SPCB	Secondary Channel B
L	Local Use
A	Access Overload Class

Screen 6: BS & Access. Info.	
SID	Current SID
NID	Current NID
DBUS	DBUS (Handsfree?)

Screen 7: BS Protocol Rev. Level	
BASE#	BASE_ID (sys par msg)
P_REV	P_REV (sync msg)
MIN_P_REV	MIN_P_REV (sync msg.

Screen 8: Time Information	
CSST	CS State
MMDDYY	Date from System Time
HHMMSS	System Time

Nokia Maintenance Display Screens (continued)

Screen 9: Acquisition Information	
TA	TADD
TD	TDROP
TC	TCOMP
TT	TTDROP
WW1	Active Window
WW2	Neighbor Window
WW3	Remaining Window

Screen 10: Active Set (#1-3)	
PPN	Pilot PN Offset
EC	Ec/Io in 1/2 db units
K	Keep? 1
PPN	Pilot PN Offset
EC	Ec/Io in 1/2 db units
K	Keep? 1
PPN	Pilot PN Offset
EC	Ec/Io in 1/2 db units
K	Keep? 1

Screen 11: Active Set (#4-6)	
PPN	Pilot PN Offset
EC	Ec/Io in 1/2 db units
K	Keep? 1
PPN	Pilot PN Offset
EC	Ec/Io in 1/2 db units
K	Keep? 1
PPN	Pilot PN Offset
EC	Ec/Io in 1/2 db units
K	Keep? 1

Nokia Maintenance Display Screens (continued)

Screen 12: Neighbor Set (#1-5)	
PPN	NBR 1 PN Offset
EC	Ec/Io in 1/2 db units
PPN	NBR 2 PN Offset
EC	Ec/Io in 1/2 db units
PPN	NBR 3 PN Offset
EC	Ec/Io in 1/2 db units
PPN	NBR 4 PN Offset
EC	Ec/Io in 1/2 db units
PPN	NBR 5 PN Offset
EC	Ec/Io in 1/2 db units

Screen 13: Neighbor Set (#6-10)	
PPN	NBR 6 PN Offset
EC	Ec/Io in 1/2 db units
PPN	NBR 7 PN Offset
EC	Ec/Io in 1/2 db units
PPN	NBR 8 PN Offset
EC	Ec/Io in 1/2 db units
PPN	NBR 9 PN Offset
EC	Ec/Io in 1/2 db units
PPN	NBR 10 PN Offset
EC	Ec/Io in 1/2 db units

Screen 14: Neighbor Set (#11-15)	
PPN	NBR 11 PN Offset
EC	Ec/Io in 1/2 db units
PPN	NBR 12 PN Offset
EC	Ec/Io in 1/2 db units
PPN	NBR 13 PN Offset
EC	Ec/Io in 1/2 db units
PPN	NBR 14 PN Offset
EC	Ec/Io in 1/2 db units
PPN	NBR 15 PN Offset
EC	Ec/Io in 1/2 db units

Screen 15: Neighbor Set (#16-20)	
PPN	NBR 16 PN Offset
EC	Ec/Io in 1/2 db units
PPN	NBR 17 PN Offset
EC	Ec/Io in 1/2 db units
PPN	NBR 18 PN Offset
EC	Ec/Io in 1/2 db units
PPN	NBR 19 PN Offset
EC	Ec/Io in 1/2 db units
PPN	NBR 20 PN Offset
EC	Ec/Io in 1/2 db units

Nokia Maintenance Display Screens (continued)

Screen 16: Candidate Set (#1-5)	
PPN	CAND 1 PN Offset
EC	Ec/Io in 1/2 db units
PPN	CAND 2 PN Offset
EC	Ec/Io in 1/2 db units
PPN	CAND 3 PN Offset
EC	Ec/Io in 1/2 db units
PPN	CAND 4 PN Offset
EC	Ec/Io in 1/2 db units
PPN	CAND 5 PN Offset
EC	Ec/Io in 1/2 db units

Screen 17-22: Task Stack Ck Info	
TASKN	Task Name
FREE	Worst-Cs Stack Free Sp

Screen 23: Stack Status Info.	
Task Stack	Overflow ind. by shift
Sys Stack	2=sys stack overflow

Screen 24: Codec Registers

The Future is Here! CDMA2000

What’s New in CDMA2000?

What's New about CDMA2000?

- CDMA2000 is the next-generation family of CDMA standards

CDMA2000 Phase I: 1xRTT

- Independent I and Q modulation almost doubles capacity, compared to old IS-95 modulation with I and Q duplication
- New types of channels are provided
    - "fundamental" channels like IS-95 traffic channels, but better coded so they require less air-interface capacity; circuit-switched
    - new "supplemental" channels can carry fast data (153K, 230K, even 307Kbps); assigned for packet bursts, not continuously
    - also optional new administrative channels for smoother operations
    - a sector can carry a dynamic "mix" of both new channel types, as well as old IS-95 traffic channels simultaneously!

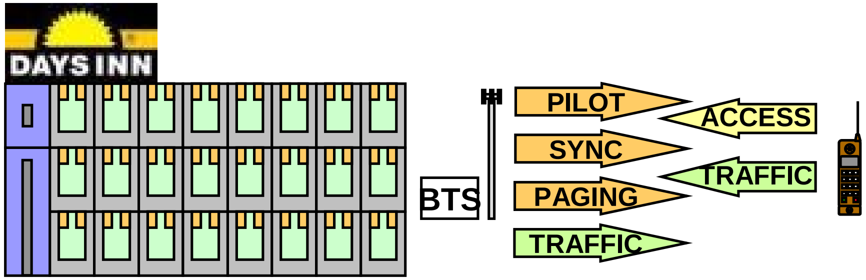
CDMA2000 Phase II: 1xEV DO, 1xEV DV, and 3xRTT

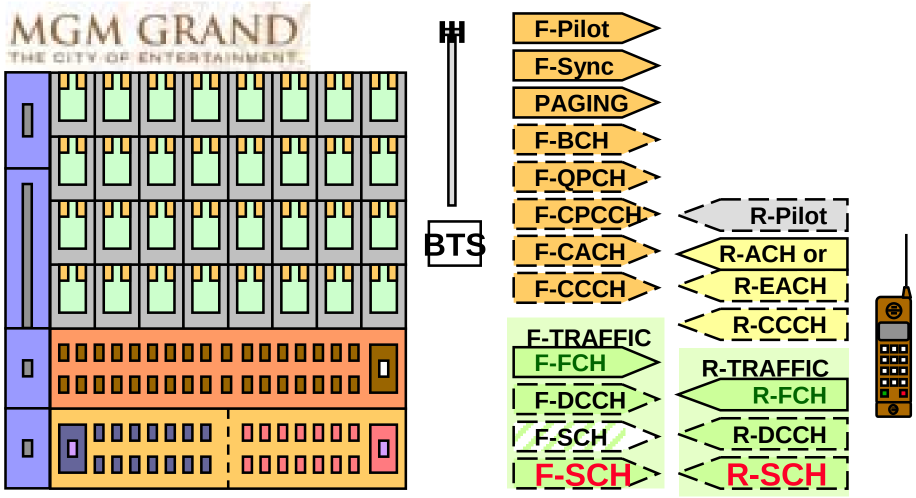
- 3xRTT: Faster data on a bundle of 3 1x carriers; probably won't be used
- 1xEV DO: 1x Evolution, Data Only (IS-856) *Qualcomm & Lucent*
    - Fast data up to 2.4 Mbps on a dedicated 1.2 MHz. CDMA Carrier
- 1xEV DV: 1x Evolution, Data and Voice "1Xtreme" *Motorola & Nokia*
    - Fast data up to 5 Mbps on a 1.2 MHz. carrier still supporting a mix of fast data and voice traffic

The CDMA Technology Path to 3G

		CDMAone		**CDMA2000/IS-2000**		
Generation	**1G**	**2G**	**2G**	**2.5G or 3?**	**3G**	**3G**
Technology	**AMPS**	**IS-95A/J-Std008**	**IS-95B**	**IS-2000: 1xRTT**	**IS-2000: 3xRTT**	**1xEV: HDR or 1Xtreme**
Signal Bandwidth, #Users	30 kHz. 1	1250 kHz. 20-35	1250 kHz. 25-40	1250 kHz. 50-80 voice and data	F: 3x 1250k R: 3687k 120-210 per 3 carriers	1250 kHz. Many packet users
Data Capabilities	None, 2.4K by modem	14.4K	64K	**153K** **307K** **230K**	**1.0 Mb/s**	**2.4 Mb/s** (HDR) **5 Mb/s** (1Xtreme)
Features: Incremental Progress	First System, Capacity & Handoffs	First CDMA, Capacity, Quality	•Improved Access •Smarter Handoffs	•Enhanced Access •Channel Structure	Faster data rates on shared 3-carrier bundle	Faster data rates on dedicated 1x RF data carrier

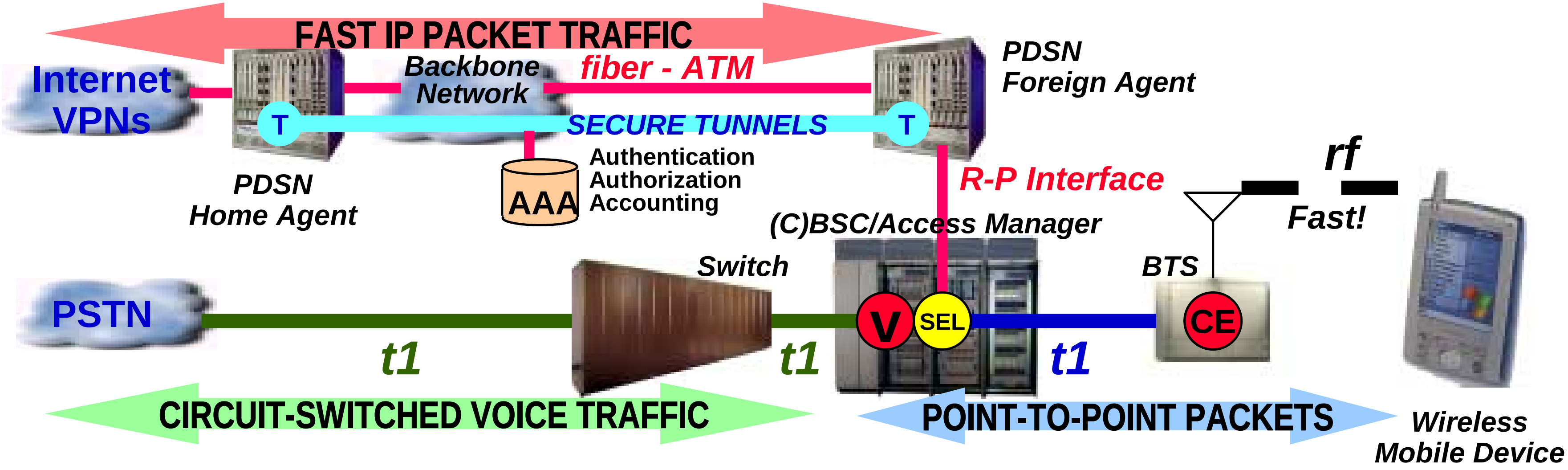
An IS-95 Sector vs CDMA2000 Sector: Cheap Hotel vs. Convention Center





- A sector on an IS-95 CDMA BTS runs like a discount hotel today
  - There's a Sign outside, a covered entranceway, Lobby
  - Only Two kinds of rooms: one king bed or two doubles
  - There are no meeting rooms or ballrooms
- New 1xRTT CDMA BTS sectors are like a convention resort!
  - Twice as big in square feet
  - Sign, Entranceway, Lobby
  - Restaurants, Bars, Nightclub
  - Guest rooms: one king bed or two doubles, maybe suites
  - Meeting Rooms with adjustable walls -- for use as Classrooms, Auditorium, Ballrooms, Banquets, Parties, Meetings

A 3G CDMA2000 1xRTT CDMA Network



- For full-featured data access over a 3G network, a true IP packet connection must be established to outside Packet Data Networks (including internet)
- This requires a Packet Data Serving Node
  - ISP and operator-provided services are provided by external Home Network and Home Agent routers
  - Authentication, Authorization, and Accounting provided by external server
- The old IWF (not shown above) is still maintained to allow old mobiles to use dial-up and WAP/wireless web keypad access

More Information on CDMA2000

- For more information on CDMA2000, download our 3G course series on www.howcdmaworks.com
  - no-cost access information is in slide #153 of this course
  - Course 331 – Introduction to 3G
  - Course 332 – Technical Details of 1xRTT
  - Course 333 – Overview of 3xRTT, 1xEV DO, 1xEV DV
  - Course 334 – 1xRTT Performance Optimization

3G Information Resources

Bibliography - Articles - Web Links

Bibliography, 3G Air Interface Technologies

“3G Wireless Demystified” by Lawrence Harte, Richard Levine, and Roman Kitka
488pp. Paperback, 2001 McGraw Hill, ISSBN 0-07-136301-7 $50. For both non-technical and technical readers. An excellent starting point for understanding all the major technologies and the whole 3G movement. Comfortable plain-language explanations of all the 2G and 3G air interfaces, yet including very succinct, complete, and rigorously correct technical details. You will still want to read books at a deeper technical level in your chosen technology, and may sometimes turn to the applicable standards for finer details, but *this* book will give you what you won’t find elsewhere -- how everything relates in the big picture, and probably everything you care to know about technologies other than your own.

"Wireless Network Evolution 2G to 3G" by Vijay K. Garg. 764pp. 2002 Prentice-Hall, Inc. ISBN 0-13-028077-1. $80. Excellent technical tutorial and reference. The most complete and comprehensive technical detail seen in a single text on all these technologies: IS-95 2G CDMA, CDMA2000 3G CDMA, UMTS/WCDMA, Bluetooth, WLAN standards (802.11a, b, WILAN). Includes good foundation information on CDMA air interface traffic capacity, CDMA system design and optimization, and wireless IP operations. Excellent level of operational detail for IS-95 systems operating today as well as thorough explanations of 2.5G and 3G enhancements.

"3G Wireless Networks" by Clint Smith and Daniel Collins. 622pp. Paperback. 2002 McGraw-Hill, ISBN 0-07-136381-5. $60. An excellent overview of all 3G technologies coupled with good detail of network architectures, channel structures, and general operational details. Good treatment of both CDMA2000 and UMTS/WCDMA systems.

“WCDMA: Towards IP Mobility and Mobile Internet” by Tero Ojanpera and Ramjee Prasad. 476pp. 2001 Artech House, ISSBN 1-58053-180-6. $100. The most complete and definitive work on UMTS (excellent CDMA2000, too!). CDMA principles, Mobile Internet, RF Environment & Design, Air Interface, WCDMA FDD standard, WCDMA TDD, CDMA2000, Performance, Heirarchical Cell Structures, Implementation, Network Planning, Basic IP Principles, Network Architectures, Standardization, Future Directions. This is a MUST HAVE for a one-book library!

More Bibliography, 3G Air Interface Technologies

“The UMTS Network and Radio Access Technology” by Dr. Jonathan P. Castro, 354 pp. 2001 John Wiley, ISBN 0 471 81375 3, $120. An excellent, well-organized, and understandable exploration of UMTS. Includes radio interface, channel explanations, link budgets, network architecture, service types, ip network considerations, a masterful tour de force through the entire subject area. Very readable, too!

“WCDMA for UMTS” by Harri Holma and Antti Toskala, 322 pp. 2000 Wiley, ISBN 0 471 72051 8, $60. Very good overall treatment of UMTS. Excellent introduction to 3G and summary of standardization activities, every level of UMTS/UTRA. Good overview of CDMA-2000, too!

“The GSM Network - GPRS Evolution: One Step Towards UMTS” 2nd Edition by Joachim Tisal, 227pp. paperback, 2001 Wiley, ISBN 0 471 49816 5, $60. Readable but not overwhelming introduction to GSM in all its aspects (140pp), DECT (11pp), GPRS (6pp), UMTS (7pp), WAP (25pp), EDGE (10pp).

Bibliography, The IP Aspect of 3G

“Mobile IP: Design, Principles and Practices” by Charles E. Perkins, 275 pp., 200, 1998 Addison-Wesley, ISBN 0-201-63469-4. $60. Comprehensive view of Mobile IP including home and foreign agents, advertisement, discovery, registration, datagrams, tunneling, encapsulation, route optimization, handoffs, firewalls, IPv6, DHCP. Tour-de-force of mobile IP techniques.

“Mobile IP Technology for M-Business” by Mark Norris, 291 pp., 2001 Artech House, ISSBN 1-58053-301-9. $67. GPRS overview and background, Mobile IP, Addressing, Routing, M-business, future prospects, IPv4, IPv6, Bluetooth & IrDA summaries.

“TCP/IP Explained” by Phillip Miller, 1997 Digital Press, ISBN 1-55558-166-8, 518pp. $50. In-depth understanding of the Internet protocol suite, network access and link layers, addressing, subnetting, name/address resolution, routing, error reporting/recovery, network management. IF you’re not already strong in TCP/IP, you’ll need this to fully master Mobile IP.

“Cisco Networking Academy Program: First-Year Companion Guide” edited by Vito Amato, 1999 Cisco Press, ISBN 1-57870-126-0, 438pp. Textbook supporting a year-long course on networking technologies for aspiring LAN/WAN (and 3G) technicians and engineers. It covers every popular networking technology (including all its elements and devices) in deep and practical detail. Excellent real-world understanding of TCP/IP, as well as the nuts-and-bolts of everything from physical components to protocols to actual devices such as routers, switches, etc. You might even want to take the evening courses at a local community college near you.

“Cisco Networking Academy Program: Engineering Journal and Workbook, Volume I” edited by Vito Amato, 1999 Cisco Press, ISBN 1-57870-126-x, 291pp. The workbook for the First Year Companion Guide above. If you want some external structure in your self-study, this workbook will hold your hand as you climb every step of the ladder, and will lead you step by step through the sister textbook, ensuring you absorb everything you need to know.

Bibliography - General CDMA

"IS-95 CDMA and CDMA2000: Cellular/PCS Systems Implementation" by Vijay K. Garg. 422 pp. 2000 Prentice Hall, ISBN 0-13-087112-5, $90. IS-95 and CDMA2000 Access technologies, DSSS, IS-95 air interface, channels, call processing, power control, signaling, soft handoff, netw. planning, capacity, data. CDMA2000 layers, channels, coding, comparison w/ WCDMA.

"CDMA Systems Engineering Handbook" by Jhong Sam Lee and Leonard E. Miller, 1998 Artech House, ISBN 0-89006-990-5. Excellent treatment of CDMA basics and deeper theory, cell and system design principles, system performance optimization, capacity issues. Recommended.

"CDMA RF System Engineering" by Samuel C. Yang, 1998 Artech House, ISBN 0-89006-991-3. Good general treatment of CDMA capacity considerations from mathematical viewpoint.

"CDMA Internetworking: Deploying the Open A-Interface" by Low and Schneider. 616 pp. 2000 Prentice Hall, ISBN 0-13-088922-9, $75. A tour-de-force exposition of the networking between the CDMA BSC, BTS, and mobile, including messaging and protocols of IS-634. Chapters on SS7, Call Processing, Mobility Management, Supplementary Services, Authentication, Resource Management (both radio and terrestrial), 3G A-Interface details. One-of-a-kind work!

"CDMA: Principles of Spread Spectrum Communication" by Andrew J. **Viterbi**. 245 p. Addison-Wesley 1995. ISBN 0-201-63374-4, $65. Very deep CDMA Theory. Prestige collector's item.

Bibliography - General Wireless

“Mobile and Personal Communication Services and Systems” by Raj Pandya, 334 pp. 2000 IEEE Press, $60. IEEE order #PC5395, ISBN 0-7803-4708-0. Good technical overview of AMPS, TACS< NMT, NTT, GSM, IS-136, PDC, IS-95, CT2, DECT, PACS, PHS, mobile data, wireless LANs, mobile IP, WATM, IMT2000 initiatives by region, global mobile satellite systems, UPT, numbers and identities, performance benchmarks.

“Wireless Telecom FAQs” by Clint Smith, 2001 McGraw Hill, ISBN 0-07-134102-1. Succint, lucid explanations of telecom terms in both wireless and landline technologies. Includes cellular architecture, AMPS, GSM, TDMA, iDEN, CDMA. Very thorough coverage; an excellent reference for new technical people or anyone wishing for clear explanations of wireless terms.

"Mobile Communications Engineering" 2nd. Edition by William C. Y. Lee. 689 pp. McGraw Hill 1998 $65. ISBN 0-07-037103-2 Lee’s latest/greatest reference work on all of wireless; well done.

Web Links and Downloadable Resources

Scott Baxter: http://www.howcdmaworks.com
Latest versions of all courses are downloadable.
Category - Username - Password
Intro - (none required) - (none required)
RF/CDMA/Performance - shannon - hertz
3G - generation - third
Grayson - telecom - allen
Agilent - nitro - viper

Dr. Ernest Simo's Space2000: http://www.cdmaonline.com/ *and* http://www.3Gonline.com/

CDG: http://www.cdg.org (check out the digivents multimedia viewable sessions)
The IS-95 and IS-2000 CDMA trade marketing webside, CDMA cheerleaders.

GSM: http://www.gsmworld.com
The GSM Association website. Worldwide GSM marketing cheerleaders but also includes some excellent GSM and GPRS technical overview whitepapers and documents; latest user figures.

UWCC: http://www.uwcc.com
The IS-136 TDMA trade marketing website, TDMA cheerleaders.

RCR News: http://www.rcrnews.com
Wireless Industry trade publication - regulatory, technical, business, marketing news.
Subscribers can access text archives of past articles; very handy in researching events.

Wireless Week: http://www.wirelessweek.com
Wireless Industry trade publication - regulatory, technical, business, marketing news.

More Web Links

3GPP: http://www.3gpp.org/
The operators' harmonization group concerned mainly with ETSI-related standards

3GPP2: http://www.3gpp2.org/
The operators' harmonization group concerned mainly with IS-95-derived CDMA standards

ITU: http://www.itu.int/imt/

ETSI: http://www.etsi.fr/

UMTS forum: http://www.umts-forum.org/

GSM MoU: http://www.gsmworld.com/

TIA: http://www.tiaonline.org/

T1: http://www.t1.org/

ARIB: http://www.arib.or.jp/arib/english/index.html

TTC: http://www.ttc.or.jp/

TTA: http://www.tta.or.kr/

ETRI: http://www.etri.re.kr/

RAST: http://www.rast.etsi.fi/