Signaling

**signaling:** exchange of messages among network entities to enable (provide service) to connection/call

- before, during, after connection/call
  - call setup and teardown (state)
  - call maintenance (state)
  - measurement, billing (state)
- between:
  - end-user <-> network
  - end-user <-> end-user
  - network element <-> network element
Examples

- SS7 (Signaling System no. 7): telephone network
- Q.2931: ATM
- GSM (Global System for Mobile communication)
- RSVP (Resource Reservation Protocol), SIP (session Initiation Protocol): Internet
Telephone Network

- created in 1876
- currently a global Infrastructure

- central office
- long haul Network
- central office
- PBX
- subscriber access lines (twisted pair)
- Toll switch (Backbone Switch)
Central Office and Local Loop

- each phone user (subscriber) has direct connection to switch in central office (local loop)
- local loop typically 1 - 10 km long
- switches in central office called (local) exchanges
- company providing local telephone service called local exchange carrier or LEC (e.g., Verizon)
PBX

- **PBX (Private Branch Exchange)** telephone system within enterprise that switches calls on local lines; allows users to share fixed number of external lines to central office
- saves cost of line per user to central office
Long-haul network

- toll switches provide long-distance connectivity over long distance trunks
- ~500 toll switches in US
- toll switch runs 100,000+ phone calls
How is voice transmitted?

Two ways:

- **analog voice transmission**: voice channel allocated bandwidth of 3.5 kHz

- **digital voice transmission**: analog voice stream converted to digital stream
  - standard scheme: 8000 8 bit samples
The digital phone network

Until 1960s:
- analog telephone network
- frequency-division multiplexing

Today:
- local loop analog
- rest of network (incl. cellular) digital (based on TDM)

When do we get all digital network?
- ISDN (Integrated services Digital Network) is all digital circuit switching technology, available since the early-1990s (in Europe) or mid-1990s (US). No wide deployment in US
- ADSL – asymmetrical digital subscriber line
- IP telephony: digital, but not circuit-switched
Analog local loop / digital network

- First telephone switch digitizes voice call (8000 8-bit samples per second)
  - Switching method is TDM.

- Switch multiplexes calls, interleaving samples in time. Call receives one 8-bit slot every 125 µs
All digital network

- telephone at subscriber digitizes voice, sends one 8-bit sample every 125 μs
Addressing and routing

- each subscriber has address (telephone number)
  - hierarchical addresses
  - example: Antonio’s Pizza in downtown Amherst

- telephone address used for setting up route from caller to callee
Telephone network: services

- point-to-point POTS calls
- special telephone numbers:
  - 800 (888,877) number service: free call to customer
  - 900 number service: bill caller
  - numbers for life
- caller ID
- calling card/third part charging
- call routing (to end user): prespecified, by time-of-day
- “follow me” service
- incoming/outgoing call restrictions
- support for cellular roaming: “home” number routed to current cell location
Telephone network: AIN

**AIN**: Advanced Intelligent (phone) Network: migration from service-in-the-switch to service logic external to (on top of) switching systems

- looks like Internet philosophy:
  - e.g., DNS is at application layer; (RIP, OSPF, BGP above IP)
- AIN advantages:
  - introduce new services rapidly
  - open interfaces: vendor customization, vendor independence of services
Telephone network: circuit-switched voice trunks (data plane)
Telephone network: data and control planes
Signaling System 7: telephone signaling network

Note: redundancy in SS7 elements
SS7: telephone network signaling

- **out-of-band signaling**: telephony signaling carried over *separate* network from telephone calls (data)
  - allows signaling between any pair of switches (not just directly-connected)
  - allows signaling during call (not just before/after)
  - allows higher-than-voice-data-rate signaling
  - security: in-band tone signaling helps phone phreaks; out of band signaling more secure

- SS7 network: *packet-switched*
  - calls circuit-switched

- lots of redundancy (for reliability) in signaling network links, elements
SS7: telephone network

- signaling *between telephone network elements*:

  signaling transfer point (STP):
  - packet-switches of SS7 network
  - send/receive/route signaling messages

  signaling control point (SCP):
  - “services” go here
  - e.g., database functions

  signaling switching point (SSP):
  - attach directly to end user
  - endpoints of SS7 network
Example: signaling a POTS call

1. caller goes offhook, dials callee. SSP A decides to route call via SSP B. Assigns idle trunk A-B

2. SSP A formulates Initial Address Message (IAM), forwards to STP W

3. STP W forwards IAM to STP X

4. STP X forwards IAM SSP B
Example: signaling a POTS call

5. B determines it serves callee, creates address completion message (ACM[A,B,trunk]), rings callee phone, sends ringing sound on trunk to A

6. ACM routed to Z to Y to A

7. SSP A receives ACM, connects subscriber line to allocated A-B trunk (caller hears ringing)
Example: signaling a POTS call

8. Callee goes off hook, B creates, sends answer message to A (ANM[A,B,trunk])

9. ANM routed to A

10. SSP A receives ANM, checks caller is connected in both directions to trunk. Call is connected!
Example: signaling a 800 call

800 number: logical phone number

- translation to physical phone number needed, e.g., 1-800-CALL_ATT translates to 162-962-1943

1. Caller dials 800 number, A recognizes 800 number, formulates translation query, send to STP W

2. STP W forwards request to M

3. M performs lookup, sends reply to A
Example: signaling a 800 call

800 number: logical phone number
- translation to physical phone number needed

1. A begins signaling to set up call to number associated with 800 number
Example: SS7 protocol stack

**TCAP:** application layer protocols: 800 service, calling card, call return, cellular roaming

**SCCP:** demultiplexing to multiple upper layer applications

**SS7-specific** network, link, physical layer protocols

- move to IP (RFC 2719)?

**ISDN end-user signaling**

**OSI Model**
- Layer 7: TCAP
- Layers 4, 5, 6
- Layer 3: SCCP
- Layer 2
- Layer 1

**SS7 Level**
- Level 4
- Level 3
- Level 2
- Level 1

**Network**
- Data Link
- Physical

**TCAP:** Transaction Capabilities Application Part
**ASP:** Application Service Part
**SCCP:** Signaling Connection Control Part
**TUP:** Telephone User Part
**ISUP:** ISDN User Part
**BISUP:** Broadband ISDN User Part
**MTP:** Message Transfer Part
Signaling: discussion

- 800 logical-number-to-physical number translations: looks like DNS
- differences?

- where is state stored?
Asynchronous Transfer Mode: ATM

- **1990’s/00 standard for high-speed** (155Mbps to 622 Mbps and higher) *Broadband Integrated Service Digital Network* architecture

- **Goal:** integrated, end-end transport to carry voice, video, data
  - meeting timing/QoS requirements of voice, video (versus Internet best-effort model)
  - “next generation” telephony: technical roots in telephone world
  - packet-switching (fixed length packets, called “cells”) using virtual circuits
Virtual circuits

“source-to-dest path behaves much like telephone circuit”

- performance-wise
- network actions along source-to-dest path

- call setup, teardown for each call before data can flow
- each packet carries VC identifier (not destination host address)
- every router on source-dest path maintains “state” for each passing connection
- link, router resources (bandwidth, buffers) may be allocated to VC (dedicated resources = predictable service)
VC implementation

*a VC consists of:*

1. *path* from source to destination
2. *VC numbers*, one number for each link along path
3. *entries in forwarding tables* in routers along path
   - packet belonging to VC carries VC number (rather than dest address)
   - VC number can be changed on each link.
     - new VC number comes from forwarding table
**VC forwarding table**

**forwarding table in northwest router:**

<table>
<thead>
<tr>
<th>Incoming interface</th>
<th>Incoming VC #</th>
<th>Outgoing interface</th>
<th>Outgoing VC #</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>12</td>
<td>3</td>
<td>22</td>
</tr>
<tr>
<td>2</td>
<td>63</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>2</td>
<td>17</td>
</tr>
<tr>
<td>1</td>
<td>97</td>
<td>3</td>
<td>87</td>
</tr>
<tr>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
</tr>
</tbody>
</table>

**VC routers maintain connection state information!**
Virtual circuits: signaling protocols

- used to setup, maintain, teardown VC
- used in ATM (we’ll study that), other architectures
- not used in today’s Internet

1. initiate call
2. incoming call
3. accept call
4. call connected
5. data flow begins
6. receive data

<table>
<thead>
<tr>
<th>application</th>
<th>transport</th>
<th>network</th>
<th>data link</th>
<th>physical</th>
</tr>
</thead>
<tbody>
<tr>
<td>application</td>
<td>transport</td>
<td>network</td>
<td>data link</td>
<td>physical</td>
</tr>
</tbody>
</table>
ATM networks
ATM Layer: Virtual Channels

- **VC transport**: cells carried on VC from source to dest
  - call setup, teardown for each call *before* data can flow
  - each cell carries VC identifier (not destination ID)
  - every switch on source-dest path maintain “state” for each passing connection
  - link, switch resources (bandwidth, buffers) may be *allocated* to VC: to get circuit-like perf.

- **permanent VCs (PVCs)**
  - long lasting connections
  - e.g., “permanent” route between two IP routers

- **switched VCs (SVC)**:
  - dynamically set up on per-call basis
ATM Signaling: Q.2931

- point to point and point-to-multipoint
- symmetric/assymmetric BW requirements
- QoS negotiation
- error recovery mechanism
ATM Signaling: Q.2931

- UNI (user-network interface)
- NNI (network-network interface)
- PNNI (private network-network interface)
- ATM network
ATM Q.2931 call setup signaling

VCI=5; VPI=0 used as signaling channel

- call reference
- addresses
- traffic spec
- QoS

- call reference
- VPI/VCI

user

UNI

ATM network

UNI

user

setup

call proc

connect

conn ack

setup

call proc

connect

conn ack

user-user data
ATM Q.2931 call release signaling

- Call reference
- Cause

Release

Release complete

- Call reference
- Cause
ATM Q.2931 call setup: timers

- timers used to recover from problems
  - 10 timers at user side, 10 timers at network side
ATM Q.2931 call release signaling

user

UNI

ATM network

UNI

user

user-user data

start T308 → release

release complete

stop T308 →

start T308 → release

release complete

stop T308 →

release complete
PNNI Signaling:

“..at a specific link, one switching system plays the role of the user side, and the other plays the role of the network side, as defined in the UNI 3.1 Specification.” ATM Forum af-pnni-0026.000
ATM signaling: discussion

- state?
- recovery?
Cellular network architecture

MSC
- connects cells to wide area net
- manages call setup (more later!)
- handles mobility (more later!)

Cell
- covers geographical region
- **base station** (BS) analogous to 802.11 AP
- **mobile users** attach to network through BS
- **air-interface:** physical and link layer protocol between mobile and BS
Cellular network architecture

BSS – Base Station System
BSC – Base Station Controller
BTS – Base Transmitter Station

radio subsystem (RSS)

Network, Switching Subsystem (RSS)

Operation subsystem (OSS)

PSTN, Internet

SS7 signaling (control)

HLR – Home Location Register
VLR – Visitor Location Register

Operations Maintenance Center

Mobile Switching Center
Gateway MSC
Cellular networks: first hop

Two techniques for sharing mobile-to-BS radio spectrum

- **combined FDMA/TDMA:** divide spectrum into frequency channels, divide each channel into time slots

- **CDMA:** code division multiple access
GSM: TDMA, FDMA structure

890-915 MHz
124 channels (200 kHz) uplink

935-960 MHz
124 channels (200 kHz) downlink

GSM TDMA frame

- **Guard**: 57 bits
- **Data**: 26 bits
- **Training**: 57 bits
- **User Data**: 57 bits

Frequency

4.615 ms

577 μs
Handling mobility in cellular networks

- **home network**: network of cellular provider you subscribe to (e.g., Sprint PCS, Verizon)
  - **home location register (HLR)**: database in home network containing permanent cell phone #, profile information (services, preferences, billing), information about current location (could be in another network)

- **visited network**: network in which mobile currently resides
  - **visitor location register (VLR)**: database with entry for each user currently in network
  - could be home network
GSM: calling a mobile

1. Call routed to home network
2. Home MSC consults HLR, gets roaming number of mobile in visited network
3. Home MSC sets up 2nd leg of call to MSC in visited network
4. MSC in visited network locates BSS containing mobile via paging, completes call through base station to mobile
GSM: handoff with common MSC

- **handoff goal:** route call via new base station (without interruption)

- **reasons for handoff:**
  - stronger signal to/from new BSS (continuing connectivity, less battery drain)
  - load balance: free up channel in current BSS
  - GSM doesn’t mandate why perform handoff (policy), only how (mechanism)

- **handoff initiated by old BSS**
GSM: handoff with common MSC

1. old BSS informs MSC of impending handoff, provides list of $1^+$ new BSSs
2. MSC sets up path (allocates resources) to new BSS
3. new BSS allocates radio channel for use by mobile
4. new BSS signals MSC, old BSS: ready
5. old BSS tells mobile: perform handoff to new BSS
6. mobile, new BSS signal to activate new channel
7. mobile signals via new BSS to MSC: handoff complete. MSC reroutes call
8. MSC-old-BSS resources released
GSM: handoff between MSCs

- **anchor MSC**: first MSC visited during call
  - Call remains routed through anchor MSC
- New MSC added to end of MSC chain as mobile moves to new MSC

(a) before handoff
GSM: handoff between MSCs

- **anchor MSC**: first MSC visited during call
  - call remains routed through anchor MSC
- new MSC added to end of MSC chain as mobile moves to new MSC

(b) after handoff
GSM: handoff between MSCs

- **anchor MSC**: first MSC visited during call
  - call remains routed through anchor MSC
- new MSC added to end of MSC chain as mobile moves to new MSC
- IS-41 allows optional path minimization step to shorten multi-MSC chain

- (b) after handoff

In GSM, handoff between MSCs involves:

- **Anchor MSC**: The first MSC visited during call.
  - The call remains routed through the anchor MSC.
- New MSC added to the end of the MSC chain as the mobile moves to a new MSC.
- IS-41 allows for an optional path minimization step to shorten the multi-MSC chain.
3G (voice+data) network architecture

- Radio network controller
- MSC
- Gateway MSC
- SGSN
- GGSN
- Public telephone network
- Public Internet

Radio interface
(WCDMA, HSPA)

Radio access network
Universal Terrestrial Radio Access Network (UTRAN)

Core network
General Packet Radio Service (GPRS) Core Network

Public Internet
3G versus 4G LTE network architecture

3G:
- Radio network controller
- MSC
- SGSN
- GGSN
- Public telephone network
- Public Internet

4G-LTE:
- MME
- HSS
- S-GW
- P-GW
- Evolved Packet Core (EPC)
- Public Internet
- Radio access network
  - Universal Terrestrial Radio Access Network (UTRAN)
4G: differences from 3G

- all IP core: IP packets tunneled (through core IP network) from base station to gateway
- no separation between voice and data – all traffic carried over IP core to gateway
Functional split of major LTE components

- **eNodeB**
  - Inter-cell RRM
  - RB control
  - Connection Mobility Control
  - Radio Admission Control
  - eNB measurement configuration and provision
  - Dynamic resource allocation (scheduler)
  - RRC
  - PDCP
  - RLC
  - MAC
  - PHY

- **MME**
  - NAS security
  - Idle state mobility handling
  - EPS Bearer Control

- **S-GW**
  - Mobile anchoring

- **P-GW**
  - UE IP address allocation
  - Packet filtering

- **Internet**

- **E-UTRAN**
  - S1

- **EPC**

- **handles idle/active UE transitions**
- **pages UE**
- **sets up eNodeB-PGW tunnel (aka bearer)**
- **holds idle UE info**
- **QoS enforcement**
Radio + Tunneling: UE – eNodeB – PGW
Radio+Tunneling: UE – eNodeB – PGW

Tunneling UE IP packet in LTE

- IP packet from UE encapsulated in GPRS Tunneling Protocol (GTP) message at ENodeB
- GTP message encapsulated in UDP, then encapsulated in IP. Large IP packet addressed to SGW
## Quality of Service in LTE

- **QoS from eNodeB to SGW:** min and max guaranteed bit rate
- **QoS in radio access network:** one of 12 QCI values

<table>
<thead>
<tr>
<th>QCI</th>
<th>RESOURCE TYPE</th>
<th>PRIORITY</th>
<th>PACKET DELAY BUDGET (MS)</th>
<th>PACKET ERROR LOSS RATE</th>
<th>EXAMPLE SERVICES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GBR</td>
<td>2</td>
<td>100</td>
<td>$10^{-2}$</td>
<td>Conversational voice</td>
</tr>
<tr>
<td>2</td>
<td>GBR</td>
<td>4</td>
<td>150</td>
<td>$10^{-3}$</td>
<td>Conversational video (live streaming)</td>
</tr>
<tr>
<td>3</td>
<td>GBR</td>
<td>5</td>
<td>300</td>
<td>$10^{-6}$</td>
<td>Non-conversational video (buffered streaming)</td>
</tr>
<tr>
<td>4</td>
<td>GBR</td>
<td>3</td>
<td>50</td>
<td>$10^{-3}$</td>
<td>Real-time gaming</td>
</tr>
<tr>
<td>5</td>
<td>Non-GBR</td>
<td>1</td>
<td>100</td>
<td>$10^{-6}$</td>
<td>IMS signaling</td>
</tr>
<tr>
<td>6</td>
<td>Non-GBR</td>
<td>7</td>
<td>100</td>
<td>$10^{-3}$</td>
<td>Voice, video (live streaming), interactive gaming</td>
</tr>
<tr>
<td>7</td>
<td>Non-GBR</td>
<td>6</td>
<td>300</td>
<td>$10^{-6}$</td>
<td>Video (buffered streaming)</td>
</tr>
<tr>
<td>8</td>
<td>Non-GBR</td>
<td>8</td>
<td>300</td>
<td>$10^{-6}$</td>
<td>TCP-based (for example, WWW, e-mail), chat, FTP, p2p file sharing, progressive video and others</td>
</tr>
<tr>
<td>9</td>
<td>Non-GBR</td>
<td>9</td>
<td>300</td>
<td>$10^{-6}$</td>
<td></td>
</tr>
</tbody>
</table>
Handling Mobility in LTE

- Paging: idle UE may move from cell to cell: network does not know where the idle UE is resident
  - paging message from MME broadcast by all eNodeB to locate UE

- handoff: similar to 3G:
  - preparation phase
  - execution phase
  - completion phase