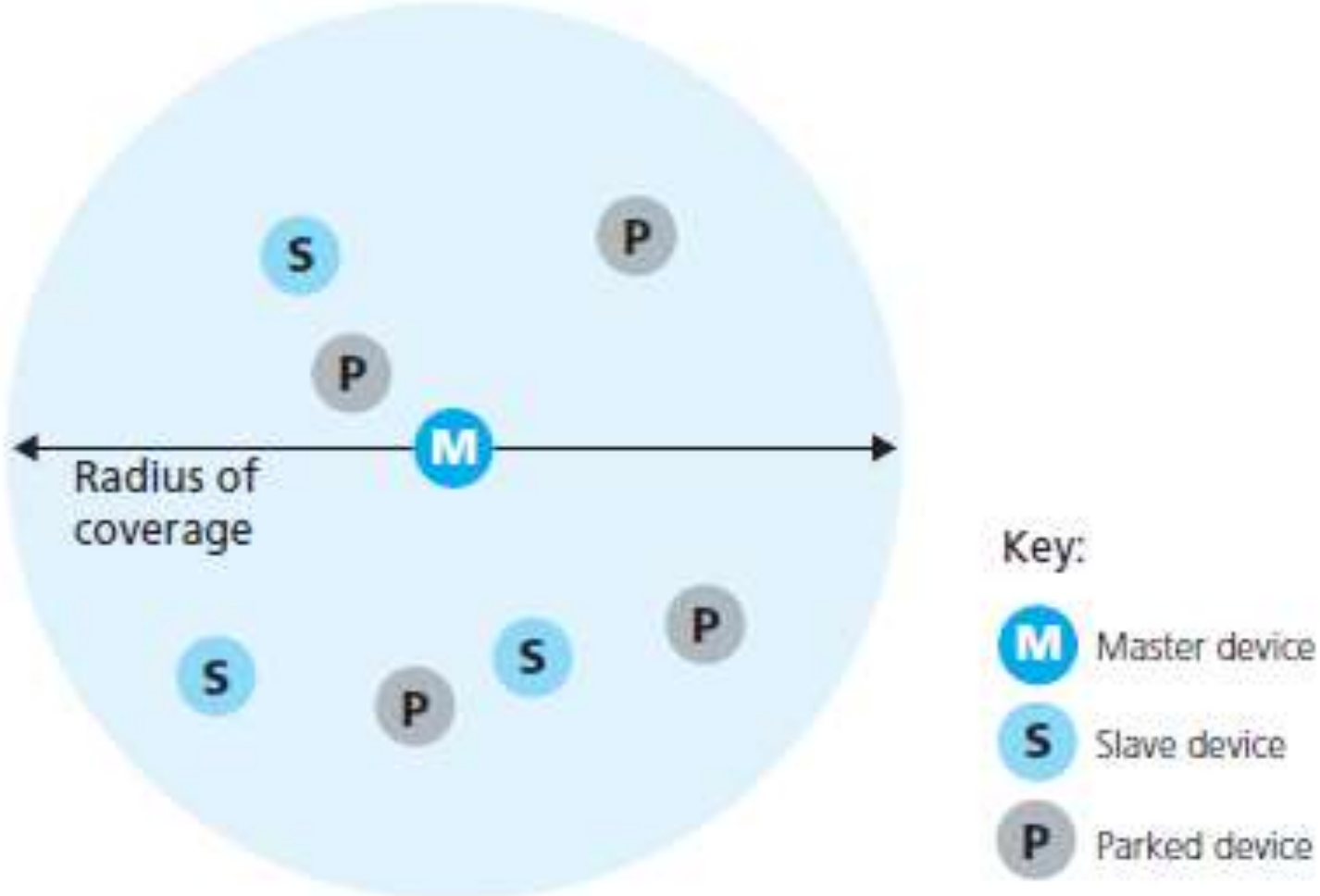
Personal Area Networks: Bluetooth and Zigbee

- The IEEE 802.11 WiFi standard is aimed at communication among devices separated by up to 100 meters.
- Two other IEEE 802 protocols are Bluetooth and Zigbee (defined in the IEEE 802.15.1 and IEEE 802.15.4 standards [IEEE 802.15 2012]) for communicating over shorter distances.
- WiMAX (defined in the IEEE 802.16 standard [IEEE 802.16d 2004; IEEE 802.16e 2005])—are standards for communicating over longer distances.

Bluetooth

- An IEEE 802.15.1 network operates over a short range, at low power, and at low cost.
- It is essentially a low-power, short-range, low-rate “cable replacement” technology for interconnecting notebooks, peripheral devices, cellular phones, and smartphones.
- For this reason, 802.15.1 networks are sometimes referred to as wireless personal area networks (WPANs).
- 802.15.1 networks operate in the 2.4 GHz unlicensed radio band in a TDM manner, with time slots of 625 microseconds.
- During each time slot, a sender transmits on one of 79 channels, with the channel changing in a known but pseudorandom manner from slot to slot.
- This form of channel hopping, known as **frequency-hopping spread spectrum (FHSS),** spreads transmissions in time over the frequency spectrum.
- 802.15.1 can provide data rates up to 4 Mbps.

- 802.15.1 networks are ad hoc networks: No network infrastructure (e.g., an access point) is needed to interconnect 802.15.1 devices.
- Thus, 802.15.1 devices must organize themselves.
- 802.15.1 devices are first organized into a **piconet** of up to eight active devices.
- One of these devices is designated as the master, with the remaining devices acting as slaves.
- The master node truly rules the piconet—its clock determines time in the piconet, it can transmit in each odd-numbered slot, and a slave can transmit only after the master has communicated with it in the previous slot and even then the slave can only transmit to the master.
- In addition to the slave devices, there can also be up to 255 parked devices in the network.
- These devices cannot communicate until their status has been changed from parked to active by the master node.



5.16 ♦ A Bluetooth piconet

Zigbee

- A second personal area network standardized by the IEEE is the 802.14.5 standard [IEEE 802.15 2012] known as Zigbee.
- Zigbee is targeted at lowerpowered, lower-data-rate, lower-duty-cycle applications than Bluetooth.
- While we may tend to think that “bigger and faster is better,” not all network applications need high bandwidth and the consequent higher costs (both economic and power costs).
- For example, home temperature and light sensors, security devices, and wallmounted switches are all very simple, low-power, low-duty-cycle, low-cost devices.
- Zigbee is thus well-suited for these devices.
- Zigbee defines channel rates of 20, 40, 100, and 250 Kbps, depending on the channel frequency.

- Nodes in a Zigbee network come in two flavors.
- So-called “reduced-function devices” operate as slave devices under the control of a single “full-function device,” much as Bluetooth slave devices.
- A full-function device can operate as a master device as in Bluetooth by controlling multiple slave devices, and multiple full-function devices can additionally be configured into a mesh network in which full-function devices route frames amongst themselves.
- Zigbee shares many protocol mechanisms : beacon frames and link-layer acknowledgments (similar to 802.11),
- carrier-sense random access protocols with binary exponential backoff (similar to 802.11 and Ethernet), and fixed, guaranteed allocation of time slots.

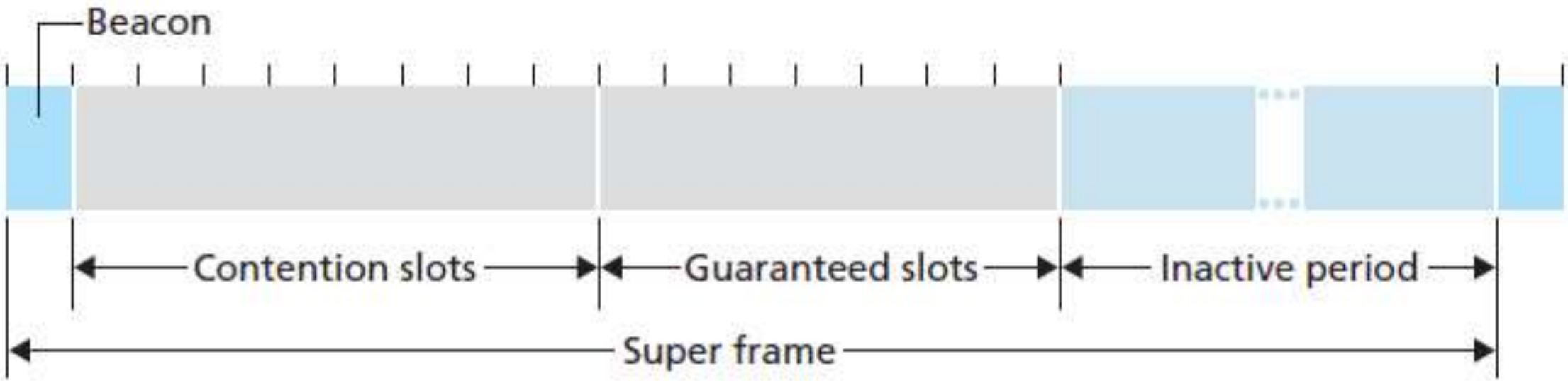


Figure 6.17 ♦ Zigbee 802.14.4 super-frame structure

- Figure 6.17 shows the case where the Zigbee network divides time into recurring super frames, each of which begins with a beacon frame.
- Each beacon frame divides the super frame into an active period (during which devices may transmit) and an inactive period (during which all devices, including the controller, can sleep and thus conserve power).
- The active period consists of 16 time slots, some of which are used by devices in a CSMA/CA random access manner, and some of which are allocated by the controller to specific devices, thus providing guaranteed channel access for those devices.

Cellular Networks

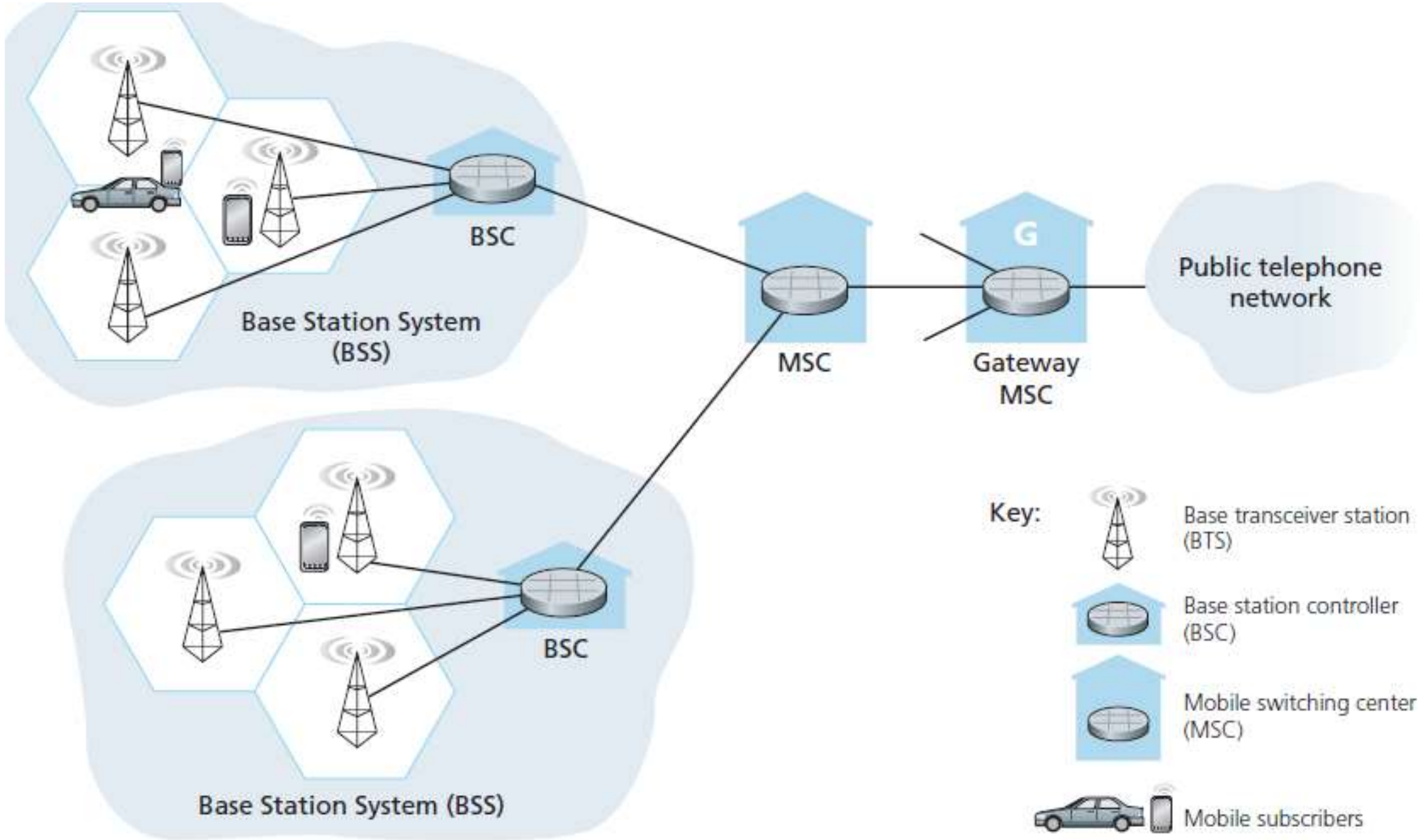
- Most WiFi hotspots have a small coverage area of between 10 and 100 meters in diameter.
- What do we do then when we have a desperate need for wireless Internet access and we cannot access a WiFi hotspot?
- A natural strategy is to extend cellular networks so that they support not only voice telephony but wireless Internet access as well.

Evolution

- The earliest generations were designed primarily for voice traffic.
- First generation (1G) systems were analog FDMA systems designed exclusively for voice-only communication.
- These 1G systems are almost extinct now, having been replaced by digital 2G systems.
- The original 2G systems were also designed for voice, but later extended (2.5G) to support data (i.e.,Internet) as well as voice service.
- The 3G systems that are being deployed also support voice and data
- Currently we have 4G,5G systems increasing emphasis on data capabilities and higher-speed.

Cellular Network Architecture, 2G

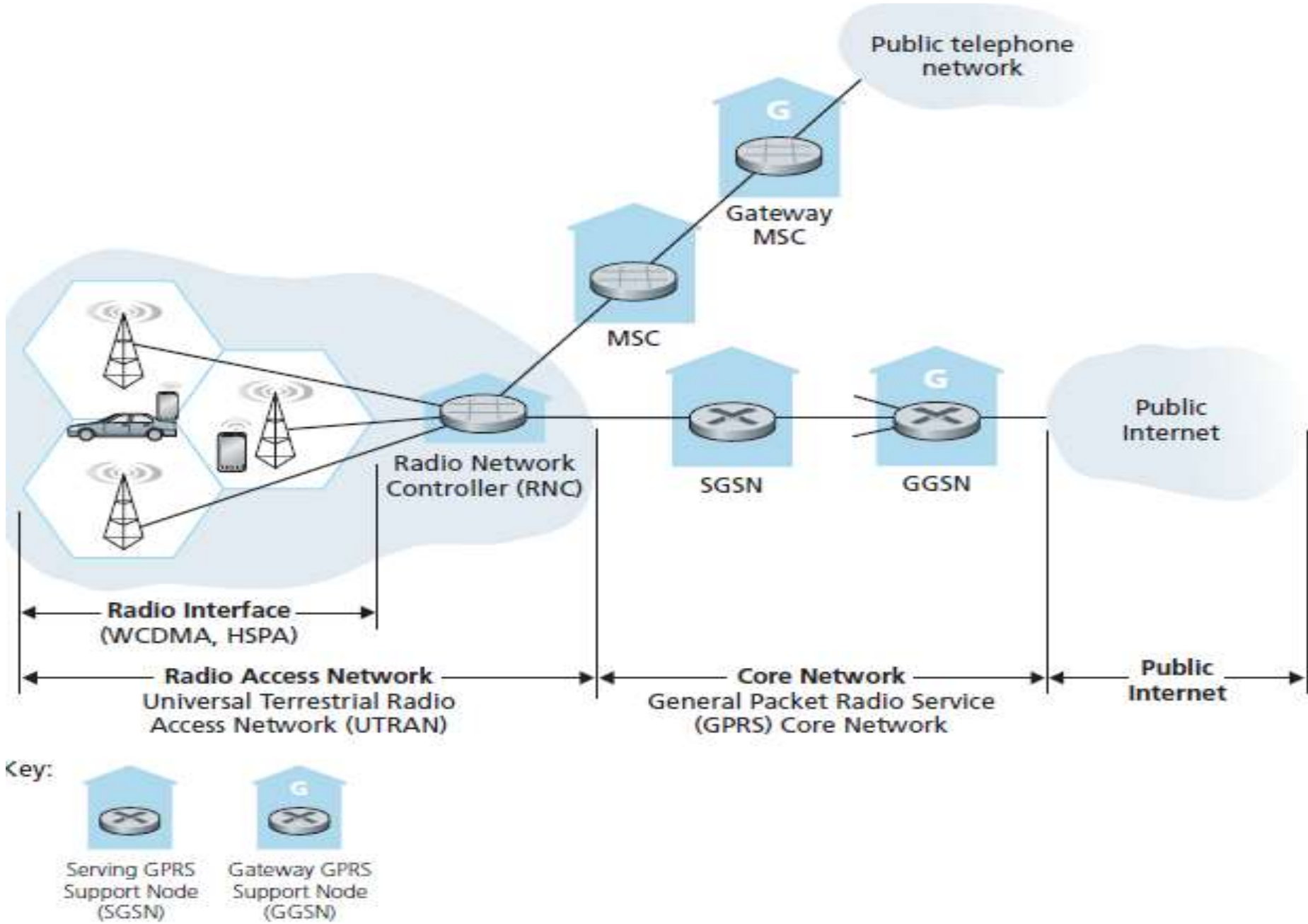
- The term *cellular* refers to the fact that the region covered by a cellular network is partitioned into a number of geographic coverage areas, known as **cells.**
- The GSM (Global System for Mobile) standard for 2G cellular systems uses combined FDM/TDM (radio) for the air interface.
- In combined FDM/TDM systems, the channel is partitioned into a number of frequency sub-bands; within each sub-band, time is partitioned into frames and slots.
- Thus, for a combined FDM/TDM system, if the channel is partitioned into *F* sub-bands and time is partitioned into *T* slots, then the channel will be able to support *F.T* simultaneous calls.


BSC
Base Station System
(BSS)
MSC
G
Gateway
MSC
Public telephone
network
BSC
Base Station System (BSS)
Key:
Base transceiver station
(BTS)
Base station controller
(BSC)
Mobile switching center
(MSC)
Mobile subscribers

- A GSM network's **base station controller (BSC)** will typically service several tens of base transceiver stations.
- The role of the BSC is to allocate BTS radio channels to mobile subscribers, perform **paging** (finding the cell in which a mobile user is resident), and perform handoff of mobile .
- The base station controller and its controlled base transceiver stations collectively constitute a GSM **base station system (BSS)**.
- The **mobile switching center (MSC)** plays the central role in user authorization and accounting (e.g., determining whether a mobile device is allowed to connect to the cellular network), call establishment and teardown, and handoff.
- A single MSC will typically contain up to five BSCs, resulting in approximately 200K subscribers per MSC.
- A cellular provider's network will have a number of MSCs, with special MSCs known as gateway MSCs connecting the provider's cellular network to the larger public telephone network.

3G Cellular Data Networks

- Extending the Internet to Cellular Subscribers.
- The 3G core cellular data network connects radio access networks to the public Internet.
- The core network interoperates with components of the existing cellular voice networks.


Public telephone network
Gateway MSC
MSC
Radio Network Controller (RNC)
SGSN
GGSN
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
Key:
Serving GPRS Support Node (SGSN)
Gateway GPRS Support Node (GGSN)

- There are two types of nodes in the 3G core network: **Serving GPRS Support Nodes (SGSNs)** and **Gateway GPRS Support Nodes (GGSNs)**.
- (GPRS stands for Generalized Packet Radio Service, an early cellular data service in 2G networks;
- An SGSN is responsible for delivering datagrams to/from the mobile nodes in the radio access network to which the SGSN is attached.
- The SGSN interacts with the cellular voice network's MSC for that area, providing user authorization and handoff, maintaining location (cell) information about active mobile nodes, and performing datagram forwarding between mobile nodes in the radio access network and a GGSN.
- The GGSN acts as a gateway, connecting multiple SGSNs into the larger Internet.
- A GGSN is thus the last piece of 3G infrastructure that a datagram originating at a mobile node encounters before entering the larger Internet.
- To the outside world, the GGSN looks like any other gateway router; the mobility of the 3G nodes within the GGSN's network is hidden from the outside world behind the GGSN.

- The 3G **radio access network** is the wireless first-hop network that we see as a 3G user.
- The **Radio Network Controller (RNC)** typically controls several cell base transceiver stations.
- Each cell's wireless link operates between the mobile nodes and a base transceiver station, just as in 2G networks.
- The RNC connects to both the circuit-switched cellular voice network via an MSC, and to the packet-switched Internet via an SGSN.
- Thus, while 3G cellular voice and cellular data services use different core networks, they share a common first/last-hop radio access network.