5G Quickstart

From “Net-head” to “Bell-head” in 20 Minutes

Joe & Drew Hess

09-FEB-2020

Overview & Goal

To Cover the Most Over-Hyped Protocol in History
To Give you just enough knowledge to be believable

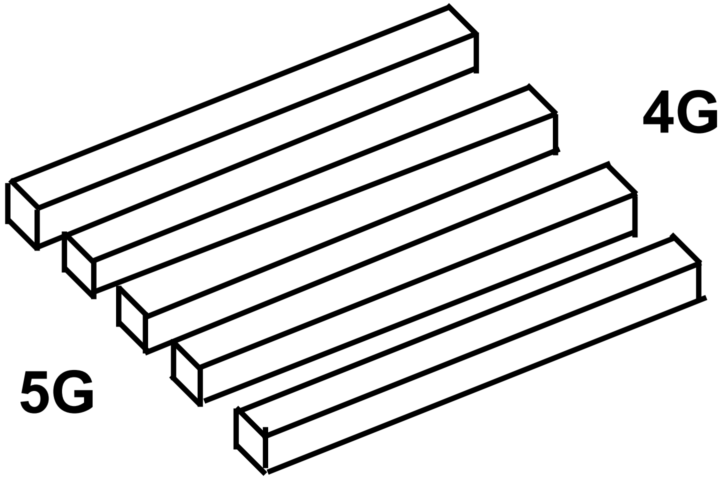
09-FEB-2020

The New Internet Explosion

- Low-cost 400Gb links
- Huge 5G rollout with new bandwidth leasing - and 5G can coexist with other mobile systems like 3G, 4G, and LTE. Existing networks can be “replanted”
- A major expansion in occurring in unlicensed low cost radio - Sigfoxx plans to sell $1 trackers early next year and have a billion customers

NANOG

What 5G Isn't



- 5Ge - really just LTE with an extra channel - this icon is displayed on many phones in use right now
- MIMO - Multiple Input-multiple Output - We already have this, but it is a component of 5G. What is coming later is coordinated multiple channels so that one data stream can be split among multiple radio links.
- CRAN - Cloud Radio Access Network - We also have this today, but it becomes a key component of 5G
- 5G is not required for self-driving cars - they are already running on LTE
- It isn't necessary for expansion of IoT, most of these will run on cheaper, unlicensed protocols. But there are applications for unlicensed 5G nets at 6.225GHz

The Basics

- Over 500 5G sites a month are being setup
- Even providers don’t even know where all are
- We can help you find the ones in your area and their capabilities, and give you some hints on managing them
- No one knows for certain how communities are going to react to 5G - for example, early complaints are that 5G phones get noticeably hot
- Consumer 5G equipment is only now becoming available in limited supply

5G is Acronym City

- 1G - Amps has maybe ten acronyms
- 2G - GPRS - Generalized Packet Radio Service uses a good fifteen acronyms
- 3G - GSM (Global System Mobile) and CDMA (Code Time Division Multiplex) -at least 25 Acronyms
- 4G - All the above plus a good fifteen more
- 5G - All the above plus a good fifty if you include all the varieties of virtualization and cloud services
- On top of this, there are more 5G organizations than all the other mobile groups put together. Any acronym beginning with 5G has a good chance of being a new organization.

Key Acronyms

- NFV - Network function virtualization.   This isn't an exclusively mobile term. It means having things like firewalls, authentication servers, and billing servers exist in a cloud, and have traffic shipped to them there, rather than having the service dedicated to a specific network section. It is necessary for virtualizaton, and allows a much simpler network configuration.
- CUPS - Combined User and Control Plane - In mobile, this is a situation where any channel can be designated a control channel.
- DSS - Dynamic Spectrum Sharing - this feature allows an operator to split mid-band spectrum between 4G LTE or 5G. This isn't the same as the sharing of radar spectrum with WiFi in the CBRS band. This is commonly used.
- NR - New Radio - A more flexible radio protocol that replaces both UMTS (3G CDMA) and LTE (4G OFDM), and allows much wider bandwidth to a RU (Radio Unit)

Quick Comparison

- This chart is oversimplified
- There is disagreement over the naming
- Different features from each generation of service may exist in other generations
- This chart ignores IS_95 & IS-2000 (CDMA One & CDMA 2000). Sprint (Now part of T-Mobile) is the largest remaining user of CDMA 2000 in the US
- LTE and NR both only support data, and encapsulate voice inside it, or downgrade the connection to an older voice service
- Frequencies are largely independent of technology except that the millimeter wave frequencies are currently only supported by 5G

Gen	Tech	Protocol
1G	FDMA	AMPS, NMT TACS
2G	CDMA	GSM
3G	W-CDMA	UMTS (3GSM)
4G	OFDM	LTE
5G	OFDMA	5G NR

Frequency Confusion

- 5G is specified on two major sets of frequencies, FR1, 410 to 7125 MHz, and FR2, 24.25 to 52.6 GHz. But AT&T's existing 5G in Las Vegas runs at about 15 GHz.
- Some of the names of the 5G bands specified by the 3GPP 5G specification also mimic IEEE names of bands. NR band N40 is called "S-Band" or "S-Band 5G", but the IEEE specifies S-band as 2-4 GHz. "L-Band" by the IEEE is 1-2 GHz, but 3GPP has three bands with "L-Band" in the name.
- There are several other NR bands in the IEEE S-Band and L-band designations to add to the possible confusion

Right Now the Press Covers 5G Rollouts

- Everything is published in newsletters and blogs, and much of it is indexed
- For example, even Bahrain is excited to announce their efforts in 5G
- One of the best public sources is the Telegeography blog https://www.telegeography.com/products/commsupdate/
- Follow these. They often list items that quickly become proprietary information, like channel bandwidth and equipment being used

NANOG

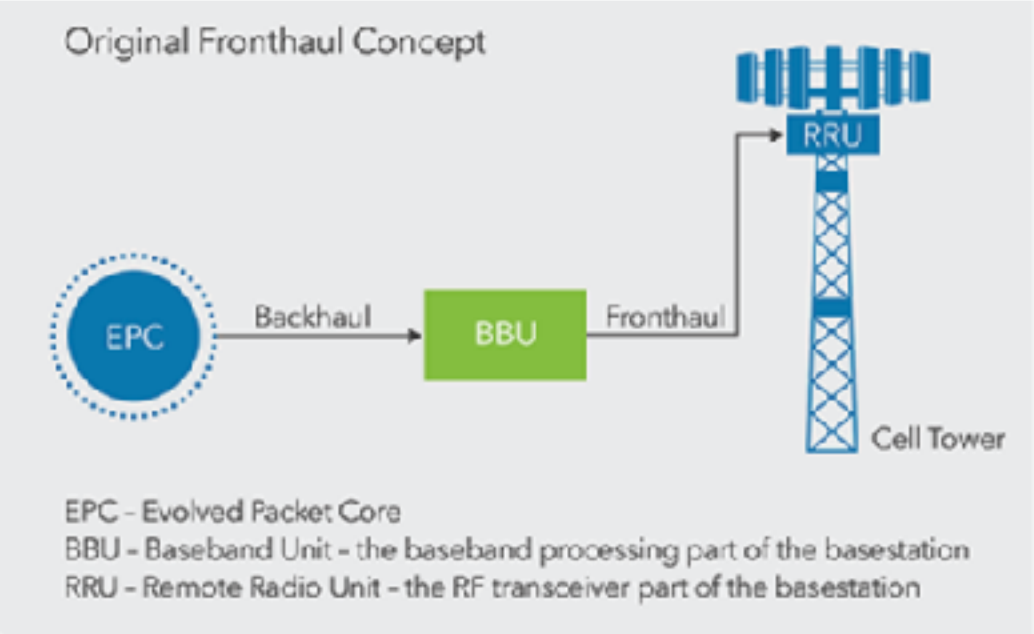
New Radio (NR) A Key 5G Component

- This is a replacement for LTE and along with it UMTS. (Universal Mobile Telecommunications Service)
- NR can run in non-Standalone mode using the LTE core. All but two commercial networks run this way today (5/2020)
- New Radio bands are shown with an “n”. For example, n258 is the 26 GHz band. They have a different structure than LTE bands, although they can be placed on top of an LTE converged core.

Why cRAN, vRAN, & oRAN?

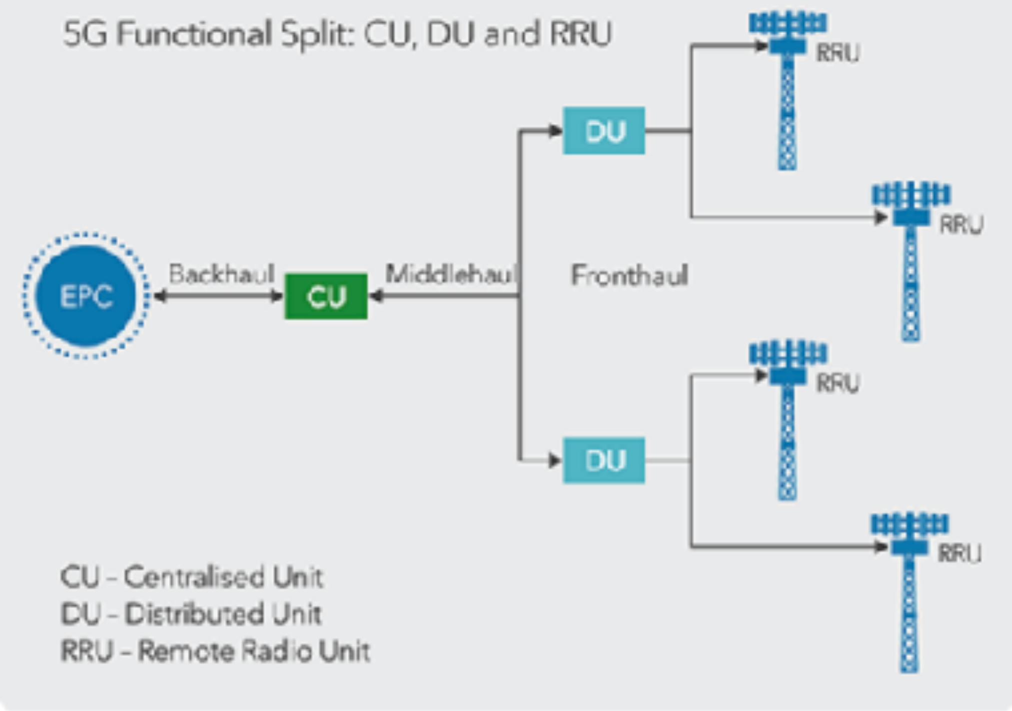
- The basics of cRAN is taking the baseband unit, the brains of a cell site, and pulling it back to a central location as opposed to having the brains sit at the tower
- This makes for smaller, cheaper towers with lower rents, and the ability to share resources for reliability
- A Virtual Radio Access Network vRAN does not have cell towers tied to specific areas, but allows their antennas to be redirected to high traffic areas
- oRAN is an Open Radio Access Network, meaning basically that any antenna can be used with any cell or phone. Most people also use the acronym to denote use of open source radio network software.

Distributed Fronthaul & CRAN



Original Fronthaul Concept

EPC - Evolved Packet Core
BBU - Baseband Unit - the baseband processing part of the basestation
RRU - Remote Radio Unit - the RF transceiver part of the basestation

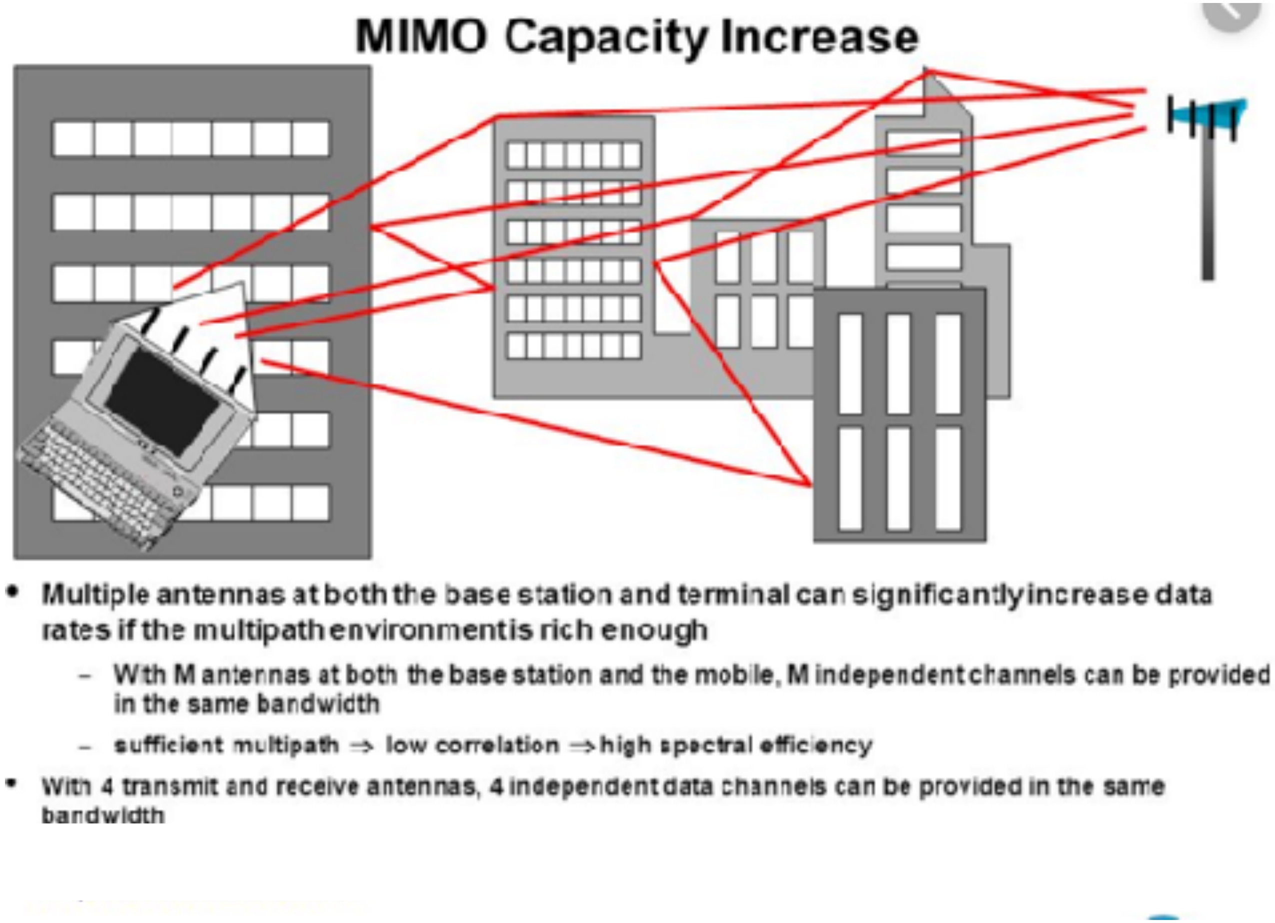


5G Functional Split: CU, DU and RRU

CU - Centralised Unit
DU - Distributed Unit
RRU - Remote Radio Unit

Taken From: https://www.spirent.com/blogs/networks/2019/october/
breakthrough-5g-experiences-exploring-fronthauls-role?
mkt_tok=eyJpIjoiWVdNM05tWXlNMkprTkRRNCIsInQiOiJqblBEVjluOHNRcG
hId3pnVjk2NjUzOStBaHNDSldQUlFzK1hwaU9FUVg2cU1VdnFBVE1iRmxcL
2hpczRpcG9SdThMUVMwNjZORGQ5T3NBXC84bndLMlJNcW10WVFFOW
ZCb2YxODNJcExiZzJhd2c2b1B4Z3JhZWRIMHVYY3lYSVY4In0%3D

MIMO - Massive In, Massive Out



MIMO Capacity Increase

- Multiple antennas at both the base station and terminal can significantly increase data rates if the multipath environment is rich enough
  - With M antennas at both the base station and the mobile, M independent channels can be provided in the same bandwidth
  - sufficient multipath → low correlation → high spectral efficiency
- With 4 transmit and receive antennas, 4 independent data channels can be provided in the same bandwidth

More on MIMO

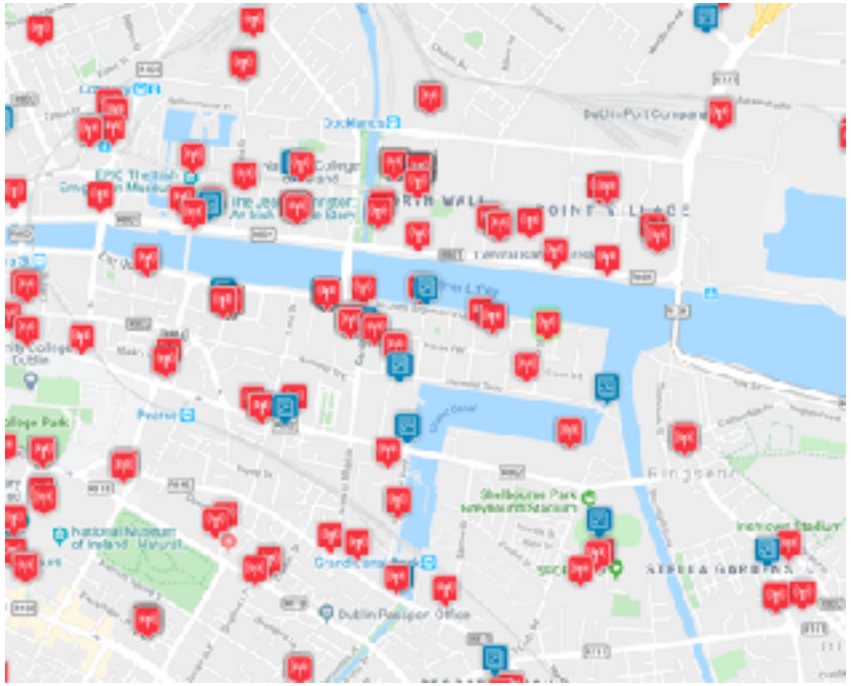
- MIMO works with 4G LTE and 5G
- Look for multiple cables leading into antennas to find a MIMO antenna
- AT&T uses 2x2 antennas with 100MHz bandwidth for its initial rollout in cities like San Francisco. You can get free service yet for a month or so (Mar 2020)

- Massive MIMO is often a planar array of 64 elements that can be individually steered in any number of ways (The antenna on left has 256 elements and is Qualcomm's test antenna)
  - They can be time-multiplexed over a neighborhood
  - They can be "ganged-together" in groups to focus energy on one mobile site
  - They can be individually steered to increase mobile unit density
  - MIMO path can be defined by polarization as well as beams

5G Maps

- There are maps galore of new mobile installations, although most are missing one or two parameters, they are helpful
- The most complete is https://www.speedtest.net/ookla-5g-map

Country Maps



Dublin's Dockyards

- Most countries also have their own tower maps for different reasons
- Ireland has a map at: https://siteviewer.comreg.ie/#site/DN991/53.3451426199/-6.2328678844/1/Site%20DN991
- There are many of these around for various reasons, consultants like siting contracts, brokers like to trade tower sites, etc.

Other Sources of Tower Data

- License lists are difficult to read, but accurate. Here is the FCC's license list page. https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp
- There is a good article that appears to be updated at:
- https://www.lifewire.com/5g-availability-world-4156244

Simple On-Site Tools

- Inexpensive SDR radios such as the Ubertooth and Hack One RF hand held radio will show what frequency the tower runs at, but you have to have a 6GHz antenna to show the S-band frequencies.   Some of these radios do not reach above 2Ghz
- You can’t see the millimeter wave sites above 10GHz without building a small test rig using a mixer. The components will cost about $800 in total
- The Qualcomm Rocket Utility plus a jail-broken Android phone will show what the phone is seeing in mobile communications

What About Phones?

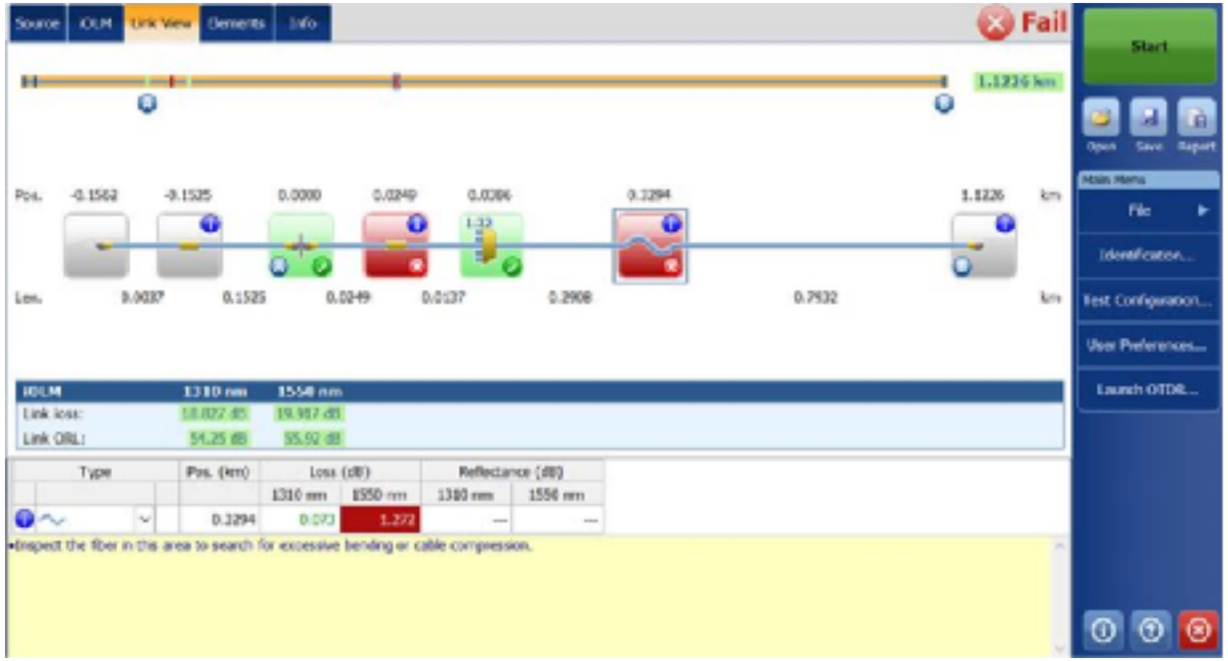
- Most end-user devices available today are hotspots and fixed end-points
- Not all 5G phones/hotspots operate on more than one or two 5G frequencies, so 5G world wide roaming is out for a while. However, most support 4G and 3G. Some support 5 or 6 frequency bands.
- A list is at: http://anisimoff.org/eng/5g/5g_devices.html

Phone Forensics

- The phone programs and applications don’t change with 5G, although are certain to be some new ones
- Existing phone forensic apps will go a long way with new 5G phones.   What they will be missing are listings of tower usage because of virtualization.
- The forensics vendors are also writing additions to their code to capture and correlate IoT sensor information. Just how they are going to do this isn’t clear.

A Good Celebrite paper:
https://privacyinternational.org/long-read/3256/technical-look-phone-extraction

Troubleshooting Fiber Connections



Pos.	-0.1562	-0.1525	0.0000	0.0249	0.0386	0.2294	1.1226	km
Len.	0.0037	0.1525	0.0249	0.0137	0.2908	0.7932		km

iOLM	1310 nm	1550 nm
Link loss:	18.027 dB	19.987 dB
Link ORL:	54.25 dB	55.92 dB

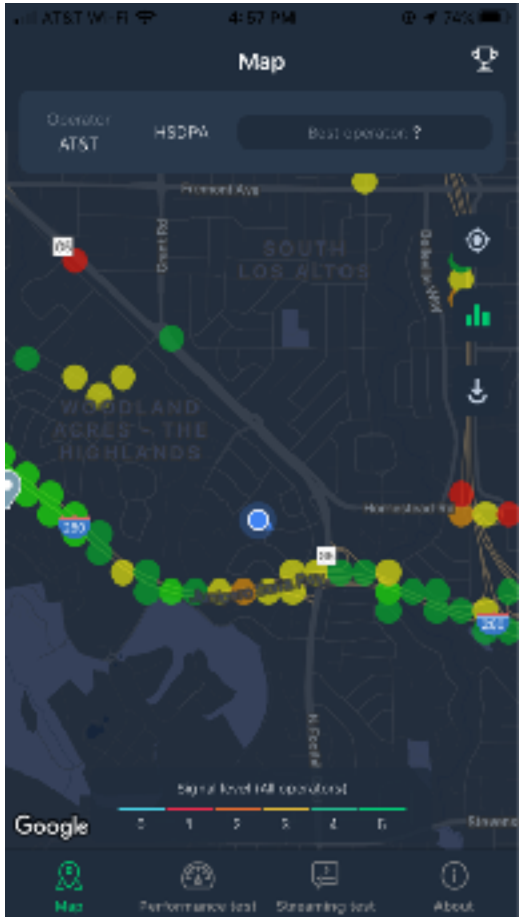
Type	Pos. (km)	Loss (dB)		Reflectance (dB)	
		1310 nm	1550 nm	1310 nm	1550 nm
∿	0.2294	0.073	1.272	—	—

•Inspect the fiber in this area to search for excessive bending or cable compression.

You will need a TDR, or Time Domain Reflectometer to effectively troubleshoot fiber connects in radio and baseband equipment. An iOLM, or Interactive Optical TDR makes this much easier. Unfortunately, they aren't cheap

Mobile Phone Based Utilities

- There are a lot of these. Some do very little more than display information in the phone’s “Settings” application. None currently support 5G. A good example is iPhone Net Analyzer, but it will let you ping something. At right is RFAnalyzer.
- Devices running Android 10 or higher can support 5G non-standalone (NSA)
- On the Android phones, there are new classes to deal with 5G. For example, CellInfoNr gives identity and measurement info



Network Issues with 5G

- 5G requires routers with high-throughput, low-latency, and best-in-class buffering
- There is a movement to move intelligence and content as close to the edge of the network as possible. There are new pieces of equipment appearing on the market using silicon like the new nVidia edge box to identify needed content through AI and store some content locally.
- 5G applications written for low latency may not work on 4G networks.
- 4G mobile applications have to be modified to run on a 5G network if it uses physical cell data.   This is also true for 3G apps today on 4G, as the programmer has to identify the type of radio used by the phone

Interview Questions & Preparations

- Does 5GPP replace 3GPP in developing 5G standards? No. The 3rd Generation Partnership Project develops 4G and 5G as well as having done work on 3G.
- Are the 5G 5 and 6 GHz bands considered millimeter wave bands? No, since they are already in use. 8 GHz is often referred to as millimeter wave although the traditional definition of millimeter waves is RF above 10GHz.
- Here is a list of all kinds of interview questions: https://www.wisdomjobs.com/e-university/5g-interview-questions.html
- The IEEE has fifteen 5G education pieces right here: https://futurenetworks.ieee.org/education/webinars

NANOG

Thank you

09-Feb-2020

HCOMM
Joe Hess - joebhess@gmail.com
Drew Hess - jondrewhess@gmail.com

NANOG