



Newsletter

What's Inside

5G is set to Take VoIP to the Next Level
Page 01

Improve VoIP Communication by Troubleshooting Common Issues
Page 02

Featured Partner: ID Agent
Page 03

Think Your Password is Secure?
Think Again
Page 04

5G is set to Take VoIP to the Next Level

Thanks to their improved speeds, greater capacity, and reduced latency, 5G networks will make VoIP even more of a must-have for businesses. Here are three ways it will do so.

MOBILE VOIP

VoIP calls rely heavily on sufficient download and upload speeds. For example, when mobile VoIP users on 4G networks are limited to 12 Mbps upload and 2 Mbps download speeds, they experience unstable and poor call connectivity and clarity. These limitations could also lead to something called packet loss, which happens when one or more "packets" of data traveling across a computer network fail to reach their destination, typically caused by network congestion. Packet loss reduces audio/video quality and could even cause calls to be dropped.

5G's greater speed prevents packet loss, but the tech has another feature that makes it better than 4G. 4G network providers set a fixed amount of bandwidth for every direction it transmits a signal to, but with 5G, the bandwidth can be adjusted on the fly.

This means that 5G network providers can allocate bandwidth to mitigate congestion as soon as it manifests itself. In practical terms, businesses could reach their customers even if the latter are in packed places that normally max out 4G mobile network capacity constraints, like in football stadiums or airports.

IMPROVED VIDEO CONFERENCING

The major factor holding web and video conferencing back is how fast current networks can transmit data. Fortunately, innovations like Web Real-Time-Communications (WebRTC) and 5G networks will enhance VoIP for businesses. Providing open and stable streaming as well as sufficient transfer speeds will soon allow businesses to accommodate higher-quality, even 4K and 8K resolution, videos.

Beyond improved streaming quality, 5G networks will also be able to support video calls with an increased number of participants. This means that businesses can serve more customers and conduct larger video meetings, which is timely, considering the current shift toward remote working.

VIRTUAL AND AUGMENTED REALITY

With 5G network speeds, virtual and augmented reality will become more common for SMBs. 5G will blow past 4G's Gbps (gigabits per second) limit, which is currently holding back the adoption of virtual reality (VR) and augmented reality (AR) applications.

VR and AR need to process significantly more data because of the visuals they must process as users move, and this puts an enormous strain on mobile networks. 5G is also set to ensure a better user experience by facilitating smoother connections and preventing network delays from affecting your bottom line.

When your business decides to adopt the up-and-coming 5G network, you can expect to see significant VoIP improvements. Ensure the success of your SMB with increased network speeds, better call quality, and conversations with consistent connectivity. ***If you're looking to set up a VoIP system for your business, call or email us today!***

Contact RJ2
(847) 303-1194

Corporate Office
1900 East Golf Rd.
Suite 600
Schaumburg, IL 60173

Chicago Office
333 S. Wabash Ave
Suite 2700
Chicago, IL 60604

Improve VoIP Communication by Troubleshooting Common Issues

Voice over Internet Protocol (VoIP) phone systems are cheaper and more efficient than regular phones, and businesses are quickly adopting it. However, transitioning without a plan can cause a range of issues that can catch business owners by surprise. Here are a few you should keep in mind.

JITTER

Jitter or crackly sounding calls result from electromagnetic interference, damaged equipment, or insufficient enough bandwidth. Here are some ways to fix this:

- Make sure the phone cables are not damaged
- Move your VoIP equipment far apart from each other to avoid electromagnetic interference
- Do a bandwidth speed test

ECHOES AND AUDIO DELAYS

Echoes and audio delays are common issues usually caused by network latency, headset lag, or the device itself. Here are tips to solve this problem:

- Make sure the device is properly plugged in and has the latest software updates.
- Unplug the phone and plug it back in. This will empty the buffers and allow the phone to re-sync with your internet connection.
- Try using a corded headset. Bluetooth headsets tend to lag, resulting in audio delays
- Make sure you have enough internet bandwidth.

DROPPED CALLS

Some users experience calls being dropped after 11 minutes. This usually happens when phones are not using the latest firmware,

or because of a user datagram protocol (UDP) timeout. Here's how to fix these issues:

- Make sure your phones are using updated firmware.
- Adjust your router settings to avoid UDP timeouts, or use Transmission Control Protocol (TCP).

CAN'T MAKE CALLS

If you're unable to make outbound calls, or if you see a big X on the VoIP phone's screen, it could mean that you're using two routers dropping critical packets of data. This issue is caused by your network layout. Disable your router's Session Initiation Protocol Application-Level Gateway (SIP ALG). You also have to make sure that you're not using two routers, as this can inhibit the flow of data packets. Another way to fix this issue is to connect your VoIP phones to a virtual local area network (VLAN).

NO SOUND

Are your calls connecting but you can't hear the person on the other line? Chances are, your firewall is blocking the Real-Time Transport Protocol (RTP) packets from coming through. To address this issue, you need to open some ports in your firewall.

CALLS ARE REDIRECTED TO VOICEMAIL

If you notice your VoIP phones are not ringing, it's possible that the calls are being redirected to voicemail. To fix this, make sure that your phone is not set to Do Not Disturb (DND) mode. Also, check if your VoIP phones are still registered with your VoIP provider.

If you need advice on installing a new VoIP system or fixing your current one, don't hesitate to call us.

RJ2 SPOTLIGHT

Ian Aureli-Braun

Business Development Representative

Ian Aureli-Braun has been in Business Development for over 5 years. Earlier in his career, Ian started building websites and mobile applications. More recently, he gained experience in sales at a telecommunications / VoIP company before joining RJ2 in May.

Ian is a raving Chicago sports fan and a proud father.

Fun fact: Ian can throw a 90MPH fastball so he's ready to bring the heat!





ID Agent provides the leading Dark Web monitoring, security awareness training and identity & access management solutions to organizations of all sizes worldwide. Its flagship product, Dark Web ID™, delivers validated intelligence to identify, analyze and monitor for compromised or stolen employee and customer data. The company's BullPhish ID™ provides cybersecurity awareness training and phishing simulation geared to the non-technical end user, to enhance a company's overall cybersecurity and further safeguard corporate systems. Passly™ delivers comprehensive identity & access management to secure remote workforces and protect organizations from risk of exposure.

www.idagent.com

Feature Partner Product: ID Agent

Dark Web ID

Dark Web ID, the Channel's number 1 dark web monitoring platform, combines intelligence with search capabilities to identify, analyze and proactively monitor for an organization's compromised or stolen employee and customer data.

BullPhish ID

BullPhish ID™ is a cybersecurity training solution that provides simulated phishing attacks and security awareness training campaigns, making your employees the best defense against cybercrime.

Passly

With Passly™, IT teams can easily, simply and affordably enable the right people to have the right access to the right resources – all from the right devices and locations. Secure Password Management, Single Sign-On, Multi-Factor Authentication and more...

Think Your Password is Secure? Think Again

The National Institute of Standards and Technology (NIST) created many of the password best practices you probably loathe — using a combination of letters, numbers, and special characters. The NIST now says those guidelines were ill-advised and has changed its stance. Find out why and what this means for you.

THE PROBLEM

The issue isn't that the NIST advised people to create easy-to-crack passwords, but their previous advice inadvertently made people create weak passwords using predictable capitalization, special characters, and numbers, like "P@ssW0rd1."

Such a password may seem secure, but the strings of characters and numbers could easily be compromised by hackers using common algorithms.

What's more, the NIST also recommended that people change their passwords regularly, but did not specify how and when to change them. Since many people thought their passwords were already secure because they've included special characters in them, most only added or changed one character.

The NIST essentially forced everyone to use passwords that are hard for humans to remember but easy for a hacker's algorithm to crack.

Eventually, the institution admitted that this can cause more problems than solutions. It has reversed its stance on organizational password management requirements, and is now recommending banishing forced periodic password changes and getting rid of complexity requirements.

THE SOLUTION

Security consultant Frank Abagnale and Chief Hacking Officer for KnowBe4 Kevin Mitnick both see a future without passwords. Both security experts advise enterprises to implement multifactor authentication in login policies.

This requires a user to present two valid credentials aside from a password to gain access to an account. This could be a code sent to the account owner's smartphone, a login prompt on a mobile device, or a facial or a fingerprint scan. This way, hackers' login efforts are futile unless they fulfill the succeeding security requirements.

Moreover, Mitnick recommended implementing long passphrases of 25 characters or more, such as "recedemarmaladecrockplacate" or "cavalryfigurineunderdoneexalted." These are much more difficult to guess and less prone to hacking. As for the frequency of changing passphrases, it will depend on a company's risk tolerance.

September

"The ultimate promise of technology is to make us master of a world that we command by the push of a button."

- Volker Grassmuck

TIPS OF THE MONTH

Optimize Your New Laptop With These Tips:

1. Update your laptop's operating system
2. Remove Bloatware
3. Install protection software
4. Optimize your power settings
5. Set up a backup plan

