Voice and Unified Communications Architecture and Design Best Practices

1 Unified Communications (UC)
   1.1 Unified Communications Overview
       1.1.1 Benefits of Unified Communications
       1.1.2 Downside of Unified Communications
   1.2 Grouping User Roles
   1.3 Physical Desk Phone
   1.4 Softphones
   1.5 Mobile
   1.6 Considerations for accessories
   1.7 Unified Communications Beyond Voice
       1.7.1 Chat/Instant Messaging
       1.7.2 Voicemail via email
       1.7.3 Presence
       1.7.4 Video
           1.7.4.1 Benefits of video integrations
           1.7.4.2 Pitfalls of integrating video

2 Analog and Digital Services
   2.1 Analog lines
   2.2 Digital lines (multi-line)
   2.3 Softphone management

3 Remote Site Voice Systems
   3.1 Options/Considerations

4 Dial Plan
   4.1 Maintenance
   4.2 Adding Area Code
   4.3 Phone numbers used for calling plans
   4.4 N11 Code Assignments
   4.5 Dial Plan Syntax
   4.6 Operator services (0)
   4.7 Calling cards
   4.8 Calling collect
   4.9 Campus (4-5 digits), local, national, international, 9xx
   4.10 10-digit dialing required for 988

5 Specialty Services
   5.1 8xx, 9xx services
   5.2 411, 311, 988 (suicide line, mandated as of 2022)
   5.3 Special events - Football, BB, Health care, campaigns
   5.4 Extension of special chts - DSL, ISDN, PRI, Analog 1FB
   5.5 Telephony/data over CBRS - private network
   5.6 Radio loops
   5.7 Point to point circuits
   5.8 Ring down - access, intercom

6 Facilities required to support voice communications
   6.1 Types of facility space
   6.2 General guidelines
   6.3 Sizing and location
   6.4 Power
   6.5 Environmental
   6.6 Access Control

7 Infrastructure support
   7.1 Certifications
   7.2 Standards

8 Data Network Design
   8.1 IP Addressing
   8.2 Power over Ethernet (PoE)
   8.3 DNS
   8.4 DHCP
   8.5 NTP
   8.6 QoS
   8.7 LLDP/CDP

9 Telemanagement Systems
   9.1 Service Tracking Tools
   9.2 Inventory of circuits, instruments, and DID’s
   9.3 Cable management
   9.4 Call Details Records
   9.5 Billing

10 Monitoring/Metrics
    10.1 SLA (Service Level Agreement(s))
       10.1.1 Cloud Services
       10.1.2 On Site Hardware
       10.1.3 Customer Provided Support
    10.2 Capacity Monitoring
       10.2.1 Capacity Management Simplified
Unified Communications (UC)

Unified Communications Overview

Voice over IP typically deals with Voice Services, whereas Unified Communications integrates multiple communications into one channel. These channels typically include voice, instant messaging/chat, fax, text messaging, and video conferencing. Common vendors that offer unified communications platforms include, Cisco, Microsoft, and Zoom.
Benefits of Unified Communications

- Improved efficiency and support through the use of a single client
- Overall cost should be lower from decoupling the communications client
- Better integration between communications channels, such as while in a video conference call, utilize chat that will live beyond the call itself
- Less administration since typically one IT support team provides all support for the UC platform
- Less learning curve for end users for common platform

Downside of Unified Communications

- Decoupling allows clients to use the best of breed solutions for each of the communications channels. For example, use cloud hosted VoIP vendors for voice services, but different vendors for collaboration and voice services
- While you lose integrations across the entire communications stack when decoupling, more vendors are supporting cross-platform integrations
- Vendor lock-in with unified communications platform. Much easier to swap out different vendors for each communications channel than to replace your entire unified communications platform

Grouping User Roles

When it comes to selecting the types of desk phones and unified communications accessories provided for faculty and staff, it’s best to group them into categories or roles. Perhaps buckets based on casual, administrative, or contact center users. While this may vary in the end, it’ll provide a good foundation for estimating the costs for your deployment and to set some basic standards.

Physical Desk Phone

While the general recommendations from a cost and portability perspective is to use softphones, physical desk phones do serve purposes, especially with contact centers. When selecting physical phones, consider the following:

- Depending on the use case, you will want to consider no display, gray, or color LED displays. Hallway phones should have no displays, casual users should have limited gray displays, and the advanced administrative or contact center staff should have the larger color displays.
- Another factor in determining the model to purchase is the number of lines for the user. Normal users may only have 1 line, whereas an administrative assistance or contact center user will have several lines.
- Consider features that are tied into the visuals or hotkeys such as unread voicemail messages, missed calls, voicemail button, and quick dial.

Softphones

If possible, softphones are generally what you should be distributing to your casual voice services users. Softphones allow for sending and receiving phone calls from any device such as computer, tablet, or mobile phone. Benefits include:

- Portability and being able to send and receive phone calls from virtually anywhere.
- Low cost, especially with laptops. In some cases, you may want to invest in headsets.
- Rich feature set
- Easier to navigate large number of contacts

Mobile

While softphones can be installed on mobile phones, another option is to just use mobile phones. The challenge here is costs and caller ID. Your institution will need to determine if they are willing to purchase cell phones for their faculty and staff. Cell phones do not show caller IDs unless the # is from a known contact.

Considerations for accessories

When it comes to unified communications, you may need to invest in accessories unless using built-in speakers, microphones, and cameras.

Headsets in particular can be challenging to standardize on and can be costly. You’ll need to consider connectivity options such as wired, wireless, and bluetooth. Styles ranging from in the ear, over the ear, and noise cancellation are available.

Consider those that have disabilities and the choices of accessories you provided them. For example, those that are hearing impair, may have difficulty hearing with certain over the ear headset or may experience discomfort.

Microphones can be built into different locations of the headset with varying voice capture quality. For those that are involved with contact centers, it is highly recommended that you use a headset with microphones that are closer to their mouths vs built into the ear piece.

With desktop, typically you’ll want to purchase cameras that mount on desktop monitors. For laptops, the recommendations change based on how the user works. For example, if it is just a laptop without any external monitors, there is no need for an external camera. Laptops with external monitors, you need to consider just using the laptop camera or mounting one on a monitor depending on where the individual will be looking at during a video conference.

Unified Communications Beyond Voice

Chat/Instant Messaging
Unified Communications typically goes beyond voice services and instant messaging is probably the most used feature. Oftentimes users will chat or instant message in lieu of phone calls because it's easier to multi-task. Functionality to look for in chat and instant messaging services.

- Ensure the chat or instant messaging system supports the basic communications features you expect them to offer such as pop-up notifications, emojis, file or document sharing, presence indicators, etc
- Saving message history
- Capability to screen share entire desktop or application
- Group chat
- Directly dial the person from the client

Voicemail via email

Most modern unified communications platforms offer features to get notified of missed calls and to listen to your voicemails. The capability and delivery of the voicemail varies depending on the platform. Minimum, you should be able to play the audio file for the voicemail directly in your email. The challenge becomes reporting back to the phone system that you have listened to the voicemail or deleted it. Well architected solutions offer this integration and it saves your users from having to delete the voicemail twice, once in email and then on the phone system.

Presence

Presence or status indicators in unified communications platforms provide users with information if someone is available to communicate with either through the phone or instant message. Presence features should include.

- Ability to manually set presence such as busy.
- Setting timer or schedule for these manually set presence indicators.
- Integrations with your calendaring systems so that when you are in a meeting, your status is automatically to in meeting or busy
- Integrations with your desktop screen sharing applications so your status is busy or do not disturb

Video

The COVID-19 pandemic dramatically increased the usage of video conferencing. In terms of unified communications, institutions need to determine whether they want to integrate video with their voice communications vendor or select a best of breed solution. In some cases, video may even be tied to your collaboration and instant messaging platform.

Benefits of video integrations

- Cost savings with negotiating with a single vendor
- Single client for all communications
- Ease of Support
- Shared contact list

Pitfalls of integrating video

- Might not get the best platform for video conferencing for all use cases such as online learning
- Vendor lock-in for all communication services makes it difficult to pivot if a newer technology fills in future needs

Analog and Digital Services

Analog lines

An analog telephone line enables, via an installed wall socket, the connection of an analog device, such as a telephone, modem or fax machine, to the telephone network. Analog line only requires a traditional two-wire cable connection. Analog line, also referred to as POTS (Plain Old Telephone Service), supports standard phones. If you see “complies with part 68, FCC Rules” and a Ringer Equivalence Number (REN), then the phone is an analog line.

Some schools and universities still provide room phones for students that connect to the campus phone system. This adds a level of security as compared to using a personal cell phone when issues arise. Most college campuses across the U.S. employ emergency blue light phones as a preeminent security feature. When someone feels unsafe on a college campus, they can push the call button on the blue tower to reach campus police. Analog phones can still remain operational even in the event of a disaster or power outage.

One of the least expensive and most secure ways to provision emergency calling in elevators and elsewhere is via analog. When the phone is accessed, caller ID information immediately transmits to an emergency center. Gateways, software, and other additional equipment are often required to provide this service through VoIP PBX service.

For the foreseeable future, expect to see analog ports persist for:

- Alarm system connections
- Telemetry systems
- Elevator and emergency phones
- Analog phones in otherwise unoccupied buildings
• Janitor and network closets
• Phone lines outside a building used to call guards for off-hours access
• Emergency phones as a lifeline to the PSTN
• Analog fax machines that operate using the T.30 standard
• TDD support for hearing impaired
• Phones in common areas that have little or no physical security
• That guard shack that is thousands of feet from any building and can be economically accessed only by an old analog line – Ethernet over CATx wiring limited to ~100ft until signal begins to dramatically degrade while analog POTS service provides both device power and dial tone over same copper pair up to 3000-5000ft, up to 10K ft possible with some equipment
• Phones in a warehouse, where installing Ethernet for a single phone is too expensive
• Dial-up PC modems, point-of-sale devices, and credit-card readers
• Intercom lines
• Announcement lines
• Access to mobile channels
• Mobile channel interconnection
• Server connections for healthcare, such as dictation, patient/bed/transport tracking, and nurse call stations
• Legacy key systems

One major advantage of an analog telephone station is cost, especially compared to IP telephone sets. This makes them ideal for common or infrequently used areas like lobbies, employee break rooms, waiting rooms, maintenance closets, and remotely located offices that require only basic calling capability.

**Digital lines (multi-line)**

A multi-line phone system allows multiple people to be on the phone at the same time. The lines can be internal or external. External lines allow you to communicate with people outside of the business, such as customers, while internal lines allow communication with your employees and colleagues.

Typically, a multi-line phone has 2, 4, or 8 speed dial buttons, some have an external additional module providing 20-24 additional speed dial buttons.

You can expect business phone systems to continue the shift to more of a unified communications system. Businesses are no longer looking for a system that only lets them make and receive calls. They want a service that also allows employees to host video calls and webinars, instant message with each other and send faxes when necessary.

Besides additional unified communications features, artificial intelligence (AI) voice analytics are another area where providers may continue to expand. New voice analytic tools will allow businesses to have their calls automatically transcribed and analyzed for certain trends. This could be a valuable tool for campuses looking to further understand the types of calls their customer service teams are fielding.

**Softphone management**

Softphone applications use a VoIP provider to make calls over the Internet through a desktop computer, tablet or smartphone. Softphone management systems range in capabilities and price, and it would be recommended to look for the following combination of features when selecting a system:

1. SaaS (Software as a Service) platform that uses call tracking and conversion intelligence to inform contact center automation—resulting in a more personalized customer experience
2. Discover which marketing campaigns are generating leads and conversions, and use that data to automate call flows and power your contact center
3. Provide remote working agility across any campus device
4. Combine enterprise-grade UC (unified communication) support for voicemail, fax, chat, and conferencing for bring your own device (BYOD)
5. Allow management for any special features, i.e. caller ID, call forwarding, intercom, auto attendant..
6. Provides provisions for tracking 911 calls either by way of locating a wifi/cellular device or by end user location self-disclosure

**Remote Site Voice Systems**

Many institutions operate smaller locations of varying sizes that are separate from their main campuses. Examples include specialized lab/research buildings, overflow office space, remote/satellite campuses, and/or shared/collaborative facilities. In some cases, these locations may be close enough to campus that it makes sense to extend the campus network with dedicated circuits and treat them just like any other campus building. In many cases, though, this is not possible because of a number of different factors including costs, distance, bandwidth limitations, local regulations, and/or specialized customer requirements.

Traditionally, the path of least resistance when it comes to telephone/voice service for these remote sites has been to simply contract with a local telephone provider to bring service to the site. While this is simple, there have been increasing levels of desire to integrate these sites with the campus telephony environment much like campus data networks can be extended by the use of technologies like site to site VPNs. Advantages of pursuing these integrated solutions include reduced digit dialing, toll cost savings, standardization of support models, and the leveraging of unified communication platforms and their associated integrated collaboration tools.

**Options/Considerations**

There are a number of options for providing main campus telephone service to remote sites. Which option you choose will depend on the available resources, anticipated use cases, and local requirements. For the most part, IP connectivity between the main campus and the remote site is assumed, but available bandwidth and the robustness/stability of the connection may play a part in the choice of deployment scenarios as well.
As a basic starting scenario, remote site users can be provisioned with soft clients and desk phones that register back to VoIP systems on the main campus, typically over a site to site VPN tunnel that services the entire remote site or through a secure proxy gateway. This provides similar use cases and support models to those of users on your main campus, and for all intents and purposes, the remote site users have an identical experience.

This is, however, completely dependent on having IP and possibly site to site VPN connectivity back to the main campus. While some softphone clients deployed on smartphones could remain in service via the cellular data network, loss of IP/VPN connectivity for the entire site could have a major impact on telephony and other operations at the remote site.

To account for this scenario, remote survivability options do exist to protect the site when it comes to telephone service. These options typically involve the installation of a small remote site gateway device to which the local telephones/clients will register in the event of not being able to communicate with the VoIP system on the main campus. The gateway is also provisioned with a backup circuit (either SIP or TDM) from a local telephone provider that will allow local devices to at least place outbound calls. Receiving inbound calls will likely require callers to dial backup numbers that are associated with the backup circuit, or, depending on the original failure scenario, having the main campus numbers assigned to the remote site users forwarded to the backup circuit.

No matter the deployment option chosen, the considerations with respect to E911 and emergency calls still apply to remote site installations. Thus, it is important to ensure that you can accurately report on location to the local PSAP and provide notifications in the event of emergency calls. You should also be aware of any differences in local/state regulations between your main campus and remote site locations.

**Dial Plan**

The International Telecommunication Union (ITU) has established a comprehensive numbering plan, designated E.164, for uniform interoperability of the networks of its member state or regional administrations. The dial plan governs the disposition of inbound and outbound calls. The dial plan typically consists of:

- Partitions, known as "dial plan rules", which are the low-level building blocks of a dial plan, specifying criteria such as dialing patterns and effective times.
- Calling profiles, which consist of one or more partitions.
- Forwarding profiles, which set global call forwarding options.
- Dial plan settings, which set calling profiles and options for internal and external users and outbound calling.

A numbering plan can specify parameters such as the following:

- **Country code**: A country code is used to reach the particular telephone system for each country or special service.
- **Area code**: An area code is typically used to route calls to a particular city, region, or special service. Depending on the region, it might also be referred to as a Numbering Plan Area, subscriber trunk dialing code, national destination code, or routing code.
- **Subscriber number**: A subscriber number represents the specific telephone number to be dialed, but does not include the country code, area code (if applicable), international prefix, or trunk prefix.
- **Trunk prefix**: A trunk prefix refers to the initial digits to be dialed in a domestic call, prior to the area code and the subscriber number.
- **International prefix**: An international prefix is the code dialed prior to an international number (the country code, the area code if any, and then the subscriber number).

**Scalable Numbering Plans**

Scalable telephony networks require well-designed, hierarchical telephone numbering plans. A hierarchical design has these five advantages:

- Simplified provisioning: Ability to easily add new numbers and modify existing numbers
- Simplified routing: Keeps local calls local and uses a specialized number key, such as an area code, for long-distance calls
- Summarization: Allows the grouping of numbers in number ranges
- Scalability: Leaves space for future growth
- Management: Control from a single management point

When designing a numbering plan, consider these four attributes to allow smooth implementation:

- Minimal impact on existing systems
- Minimal impact on users of the system
- Minimal translation configuration
- Consideration of anticipated growth

Although a non-overlapping numbering plan is usually preferable to an overlapping numbering plan, both plans can be configured to be scalable.

**Maintenance**

In MS Teams (a cloud provider instance), there are two types of dial plans: service-scoped and tenant-scoped (which is for your organization).

A service-scoped dial plan is defined for every country or region, where Phone System is available. Each user is automatically assigned the service country dial plan that matches the usage location assigned to the user. You can’t change the service country dial plan, but you can create tenant scoped dial plans, which augment the service country dial plan. As clients are provisioned, they obtain an “effective dial plan,” which is a combination of the service country dial plan and the appropriately scoped tenant dial plan. Therefore, it’s not necessary to define all normalization rules in tenant dial plans as they might already exist in the service country dial plan.
Tenant dial plans can be further broken into two scopes - tenant-scope or user-scope. If a tenant defines and assigns a user-scoped dial plan, that user will be provisioned with an effective dial plan of the user’s service country dial plan and the assigned user dial plan. If a tenant defines a tenant-scoped dial plan but doesn’t assign a user-scoped dial plan, then that user will be provisioned with an effective dial plan of the user’s service country dial plan and the tenant dial plan.

Adding Area Code

A common task for system administrators is to configure their system to recognize new area codes or prefixes.

Many telephone numbering plans are structured based on divisions into geographic areas of the service territory. Each area identified in the plan is assigned a numeric routing code. This concept was first developed for Operator Toll Dialing of the Bell System in the early 1940s, which preceded the North American Numbering Plan of 1947. The North American Numbering Plan (NANP) divided the North American service territories into numbering plan areas (NPAs), and assigned to each NPA a unique numerical prefix, the numbering plan area code, which became known in short-form as area code. The area code is prefixed to each telephone number issued in its service area.

National telecommunication authorities use various formats and dialing rules for area codes. The size of area code prefixes may either be fixed or variable. Area codes in the NANP have three digits.

Area codes by state in USA can be found here: https://www.allareacodes.com/area_code_listings_by_state.htm

Phone numbers used for calling plans

Administrators configure different telephone number types depending on the purpose for which you want to use the phone number. The two main categories are user numbers, which can be assigned to users in your organization, and service numbers, which are assigned to services such as Audio Conferencing, auto attendants, or call queues.

- User numbers are assigned to users, and there are two kinds:
  - Geographic numbers have a relationship to a geographic area and are the most common. For example, geographic phone numbers in most cases can only be used within a certain address, city, state, or region of the country.
  - Non-geographic numbers Non-geographic numbers are national numbers that don’t have a relationship to a geographic area within a country/region. For example, non-geographic numbers often have the same cost when calling the number from anywhere within the country/region. Also, some countries, such as Denmark, only have non-geographic numbers available.
- Service numbers Service numbers are available in several different number types, and availability does vary by country/region.
  - Toll service numbers
    Toll service numbers may incur a toll cost to the caller, and there are two kinds:
    - Geographic numbers Geographic numbers have a relationship to a geographic area. For example, geographic phone numbers in most cases can only be used within a certain address, city, state, or region of the country.
    - Non-geographic numbers Non-geographic numbers are national numbers that don’t have a relationship to a geographic area within a country/region. For example, non-geographic numbers often have the same cost when calling the number from anywhere within the country/region.
  - Toll-free service numbers These service numbers don’t typically incur a toll cost to the caller. Teams provides national toll-free numbers in over 60 countries/regions.

N11 Code Assignments

Eight N11 codes, called service codes, are not used as area codes. These are three-digit codes in the N11 format, as shown below:

211 - Community information and referral services (United States)
311 - Non-emergency police and other governmental services (United States)
411 - Local directory assistance
511 - Traffic and transportation information (United States); reserved (Canada)
611 - Repair service
711 - Telecommunications relay services (TRS)
811 - Access to One Call Services to Protect Pipeline and Utilities from Excavation Damage (US)
911 - Emergency

In some U.S. states, N11 codes that are not assigned nationally can be assigned locally, if the local assignments can be withdrawn promptly if a national assignment is made. There are no industry guidelines for the assignment of N11 codes.

Additional NANP reserved area codes include the following:

- 456-<2–9>XX-XXXX numbers: These codes identify carrier-specific services by providing carrier identification within the dialed digits. The prefix following 456, <2–9>XX, identifies the carrier. Use of these numbers enables the proper routing of inbound international calls, destined for these services into, and between, NANP area countries.
- 555-01XX line numbers: These numbers are fictitious telephone numbers that can be used, for example, in the film industry, for educational purposes, and for various types of demonstrations. If anyone dials one of these numbers, it does not cause a nuisance to any actual person.
- 800-XXXX through 855-XXXX line numbers: These numbers are in the format 800-855-XXXX and provide access to PSTN services for deaf, hard-of-hearing, or speech-impaired persons. Such services include Telecommunications Relay Service (TRS) and message relay service.
• 900-02–9XX-XXXX numbers: These codes are for premium services, with the cost of each 900 call billed to the calling party. 900-02–9XX codes, each subsuming a block of 10,000 numbers, are assigned to service providers who provide and typically bill for premium services. These service providers, in turn, assign individual numbers to their customers.

Dial Plan Syntax

Analog telephone adapters, IP phones, and many other VoIP media gateways have configuration options that establish the digit sequences that can be dialed with the equipment. The dial plan of these devices is established by a digit map. The following syntax may be used for such dial plan, as adapted from RFC 2705, the specification for the Media Gateway Control Protocol.

Operator services (0)

Operator assistance refers to a telephone call in which the calling party requires an operator to provide some form of assistance in completing the call. Operator-assisted calls can be more expensive than direct dial calls. In the Bell System, an operator-assisted call had a 50% premium, but only on the initial period, usually 3 minutes.

Operator-assisted numbers in North America (North American Numbering Plan): 0 (local), 00 (national non-local), 01 (international).

Calling cards

Prepaid phone cards can be purchased and used for a flat fee to make long distance telephone calls. Cards provide you a specified amount of call time to certain destinations. For example, advertisements for these cards may offer "$5 for 1000 Minutes to Guatemala."

After purchasing a card, you use it by calling an access number, which can be either a local telephone number or a toll-free number. You will then be prompted to provide your personal identification number, usually listed on the card you purchased, and the telephone number you wish to call. An automated voice may tell you how much time you have left on your card, as well as give you other information or options.

When buying a prepaid phone card, be sure you fully understand all of the instructions, fees, terms and conditions. Make sure you:

• Read the fine print on the packaging or back of the card to understand any conditions or limitations on the use of the card.
• Understand the rates for your particular phone card and any fees that may be assessed to use the card. In some cases the card's value will be reduced by "post-call," "disconnect" or "hang-up" fees after each time you use the card, or by a "maintenance" fee charged after you use the card for the first time and again at regular intervals.
• Check whether the advertised minutes for the card apply only to a single call or if the minutes can be used for multiple calls.
• Check the card's expiration date to avoid losing unused minutes.
• Look for a toll-free customer service number provided with or on the card, and make sure you will not be charged for calling it.
• Ask your friends and family to recommend cards they liked using.

Beware of false advertising!

Ads from certain prepaid card providers claim that buyers can make hundreds or thousands of minutes of calls to certain advertised destinations for just a few dollars. In reality, a consumer using these particular cards could make calls for only a fraction of those minutes due to multiple hidden fees and surcharges. In 2015, the FCC fined six companies $30 million for deceptive marketing of calling cards.

Common complaints associated with prepaid phone cards:

• Access numbers and/or PINs don’t work.
• Service or access numbers are always busy.
• Card issuers go out of business, leaving people with useless cards.
• Rates are higher than advertised, or contain undisclosed fees.
• Undisclosed "post-call" fees deducted after a call's completion.
• Undisclosed "maintenance" fees deducted after a call or at regular intervals.
• Cards charge you even when your call does not go through.
• Poor quality connections.
• Cards expire without the purchaser’s knowledge.
• Per-call fees deducted from the call time.

What should I do if I have a problem with a prepaid phone card?

First, try calling the customer service number listed on the card. If you’re unable to contact the card issuer, you can file a complaint with the FCC.

Other problems?

If you are having a problem with the local retailer from which you purchased the card, try calling or writing your local Consumer Affairs or Better Business Bureau or state Attorney General. These phone numbers are often found in the blue pages or government section of your local telephone directory.

Prepaid phone cards are often marketed by companies other than the telephone company or service provider. If you have concerns about deceptive or false advertising or marketing practices, contact the Federal Trade Commission: www.consumer.ftc.gov.

Calling collect
A Collect call is a telephone call that is paid for the person receiving the call instead of the person making the call. To place a collect call, the caller must first request that a collect call be placed (either by speaking to an operator or automated attendant), then they dial the number of their friend/loved one.

It is generally possible to make a collect call from a landline by dialing "0" and following automated prompts or using operator assistance. The receiving party must agree to the charges (usually after being informed of the name of the caller) before the call can continue normally. In general, customers can configure their landline or cell phone account to block attempted collect calls. Because the name of the caller is given before charges are accepted, it is possible to communicate a simple message for free by giving an agreed-upon name or simply using the call to synchronize an action (e.g. indicating it is time to meet). This is, however, considered toll fraud and can be prosecuted, although in most cases it is probably unlikely the person could be caught.

AT&T no longer operates a collect call service for the United States.

Verizon terminated the ability to receive collect calls on its landlines in 2016.

Campus (4-5 digits), local, national, international, 9xx

Dialing Habits:

4- or 5-digit intra-site
+ dialing for dialing from directories
US sites
9 + 7-digit for local calls
91 + 10-digit for national calls
9011 for international calls

Dial Plan Scalability Issues in Large Networks:

- Call routing information between separate call routing domains has to be manually configured:
  - Full-mesh configuration - Extremely complex, only suitable for small networks
  - Hub-and-spoke configuration when using centralized call routing entities (SIP network services or H.323 gatekeepers) - Scales better than full-mesh topologies. Requires redundant deployment of central services
- Changes have to be manually configured
- PSTN backup has to be implemented independently at each call routing domain
- No dynamic exchange of call routing information, no automatic PSTN backup

Scalable Dial Plan Solution for Large Networks

- Solutions for dynamic exchange of routing information exist
  - Dynamic IP routing protocols
    - Routers have local networks attached
    - Routers advertise local networks to other routers
    - All routers learn all available networks and how to get there
- Same concept can be used for call routing information
  - Call routing domains advertise telephone numbers or number ranges
    - Internal numbers and IP address for VoIP
    - External numbers for PSTN backup

10-digit dialing required for 988

988 is not a nationwide calling code right now.

The rules require phone service providers to direct all 988 calls to the existing National Suicide Prevention Lifeline by July 16, 2022. During the transition to 988, Americans who need help should continue to contact the National Suicide Prevention Lifeline by calling 1-800-273-8255 (1-800-273-TALK) and through online chats. Veterans and Service members may reach the Veterans Crisis Line by pressing 1 after dialing, chatting online at www.veteranscrisisline.net, or texting 838255.

The new rules will apply to all telecommunications carriers as well as all interconnected and one-way Voice over Internet Protocol (VoIP) service providers. They provide for a two-year transition, reflecting the nature of this nationwide effort, including the need for network changes and providing time for the National Suicide Prevention Lifeline to prepare for the expected increase in the volume of calls. Under these rules, calls to 988 will be directed to 1-800-273-TALK, which will remain operational during the 988 transition and after it is completed.

To ensure that calls to 988 reach the National Suicide Prevention Lifeline, all covered providers will be required to implement 10-digit dialing in areas that both use seven-digit dialing and use 988 as the first three numbers in seven-digit phone numbers.

Timeline for Transition to 10-Digit Dialing:

Beginning April 24, 2021, to begin to become accustomed to 10-digit dialing, consumers should begin dialing 10 digits (3-digit area code + 7-digit telephone number) for all local calls. If they forget and dial just 7 digits, their call will still be completed.
Beginning October 24, 2021, consumers must dial 10-digits (area code + telephone number) for all local calls. On and after this date, local calls dialed with only 7 digits may not be completed, and a recording will inform you that your call cannot be completed as dialed. Consumers must hang up and dial again using the area code and the 7-digit number.

Beginning July 16, 2022, dialing “988” will route calls to the National Suicide Prevention Lifeline.

Call 1-800-273-8255 to reach the National Suicide Prevention Lifeline today.

Veterans should Press 1 to be connected with the Veterans Crisis Line.

**Specialty Services**

8xx, 9xx services

1. 800 services for incoming to a DIT – direct inward termination
2. 800 outward dials
3. 800 inwards to DID number (conversion for University purposes)

411, 311, 988 (suicide line, mandated as of 2022)

1. Specialty codes used for directory assistance, information, now new requirement for 988

Special events - Football, BB, Health care, campaigns

1. Events that cover many aspects of telecommunications that the telecommunications department provides

Extension of special ckts - DSL, ISDN, PRI, Analog 1FB

1. Special extension of these services
2. Dial tone, PRI, T1, DSL, ISDN like circuits for NON University agencies – sporting, radio, etc

Telephony/data over CBRS - private network

1. New generation of Citizens Broadband Radio Service for public and private LTE networks for the future in higher education

Radio loops

1. From radio stations – ESPN like, local loops for connections for special events

Point to point circuits

1. Extension of T1, DSL- ADSL, HDSL, Pairgain over copper or fiber plant

Ring down - access, intercom

1. Access control for ring down for security, compliance

**Facilities required to support voice communications**

Telecommunication facilities are spaces and secured rooms containing telecommunication, network, and data processing equipment. These secured rooms have stringent requirements due to the expense and complexity of the equipment housed in them that supports the network and telecommunications infrastructure.

**Types of facility space**

Equipment Room (ER) provides centralized spaces for telecommunication, network, and data processing equipment. It is the demarcation between the distribution layer and the building’s entrance cabling.

Entrance Facility / Main Distribution Frame (EF/MDF) provides the main telecommunications and network service entrance into the building. It is the area where demarcation between the building entrance and intra-building cabling systems is affected.
Telecommunication Room / Intermediate Distribution Frame (TR/IDF) provides for demarcation between floor horizontal customer service cabling and the building service backbone. Telecommunication Rooms are allocated to each floor of a building and contain the equipment and related wiring that serves that specific floor. Several TR/IDFs may be located on a single floor in order to maintain the cable length limitations specified with TIA/EIA-569 standards.

General guidelines

All work associated with Equipment Rooms, Entry Facilities, and Telecommunication Rooms shall comply with the National Electrical Code, state and local building codes. The guidelines developed by ANSI/TIA/EIA, BICSI, and ASHRAE shall also be followed in both design and construction.

No plumbing, HVAC or electrical conduit shall pass through or above the rooms, except for sprinkler systems. Sprinkler heads shall be caged.

Under no circumstances shall electrical, fire alarm or any other utility panel be located in the rooms.

Wall Mounted Fire System Strobes - Cable tray installed in the rooms mount at a height ~7' AFF. As an unoccupied space, these rooms shall have any required fire system wall mounted strobes mounted below the cable tray.

Ceilings - The minimum ceiling height should be 9’ above finished floor (AFF). Consideration should be given to having a 10’ AFF height. There will be no suspended ceilings in the rooms. The ceiling finish should minimize dust and be light colored to enhance room lighting.

Floors - Floor loading must be at least 50 pounds per square foot (50lb/ft²). The preferred floor covering shall be vinyl composition tile (VCT). Sealed concrete will also be an option with approval. Carpets are prohibited in any Telecommunication Facility.

Lighting - Minimum lighting to be equivalent to 540 lux (50 foot-candles) measured 3 feet AFF. Lighting fixtures should be a minimum of 8.5 feet AFF when possible. Provide electrical power for the lighting, which should not come from the same circuits as the telecommunications equipment. Light switches shall be located near the entrance to the telecommunication space.

Sizing and location

Equipment Room (ER) - The ER locations shall be distributed in multiple locations for redundancy and located in the basement or bottom floor of the building.

The ER shall be rectangular in shape and not be less than 10’x18’.

Entrance Facility (EF/MDF) - The EF shall be centrally located in the basement or bottom floor of the building whenever possible. The TR/IDFs shall be stacked above the EF to allow for ease of cable distribution and cable distances. The EF shall receive two (2) 4” EMT conduits that feed directly into the building utility entrance or tunnel system.

The EF shall be rectangular in shape and not be less than the following size, depending on the total building area being served.

<table>
<thead>
<tr>
<th>Area Range</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>10,000 to 50,000 sq. ft</td>
<td>10’x8’ Mini</td>
</tr>
<tr>
<td>50,000 to 100,000 sq. ft</td>
<td>10’x12’ Small</td>
</tr>
<tr>
<td>100,000 to 150,000 sq. ft</td>
<td>10’x15’ Normal</td>
</tr>
<tr>
<td>150,000 to 200,000 sq. ft.</td>
<td>10’x18’ Large</td>
</tr>
</tbody>
</table>

Telecommunication Room (TR/IDF) - There shall be at least one, centrally located, TR per floor. Telecommunication Rooms shall not be located in a way that forces access to be used through a mechanical space. The maximum distance between the rack in the TR to the telecommunication field outlet shall not exceed 90m (295’), as measured per the cable pathway.

The TR shall be rectangular in shape and not be less than the following size, depending on the total building area being served.

<table>
<thead>
<tr>
<th>Area Range</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000 sq ft. or less</td>
<td>6’x6’ Mini</td>
</tr>
<tr>
<td>5,000 to 8,000 sq. ft</td>
<td>10’x8’ Small</td>
</tr>
<tr>
<td>8,000 to 10,000 sq ft</td>
<td>10’x11’ Normal</td>
</tr>
</tbody>
</table>

Power

Equipment Room (ER) - Redundant power circuits shall be provided with Power Distribution Units (PDU’s) installed in each rack to allow equipment to operate on either A or B power feeds. All equipment shall have redundant power supplies which are connected into the A and B PDU’s. For any equipment with only one power supply, the device shall be configured in redundant pairs, with each connected to a different power feed, or connected to an Automatic Transfer Switch (ATS) to facilitate power redundancy.

The power feeds shall be UPS protected, with at least n+1 redundancy, as well as protected with backup generator power. Monthly failover and generator tests shall be performed.

Entrance Facility (EF/MDF) and Telecommunication Room (TR/IDF) - Shall have one (1) 20Amp, 120V double duplex convenience outlets on 3 of the 4 walls. A 4th double duplex 20Amp, 120V outlet on an emergency power circuit shall be provided for wall mounted control panels. A dedicated emergency duplex 20Amp, 120V circuit shall have a demarcation in a ceiling mount 4-11/16” square electrical box.

Each room circuit shall be protected with an appropriately sized UPS to provide at least 1 hour of runtime.
Environmental

Planning for and designing the cooling and air management systems shall refer to the standardized operating environments for IT equipment set forth by the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE). The general guidelines shall be to maintain a room temperature of 65 to 75 degrees with 35-55 percent humidity control with the full complement of equipment in the room. The rooms shall also maintain a positive pressure with a minimum of one air change per hour.

The below chart identifies the recommended and alternative cooling systems options, based on total load.

<table>
<thead>
<tr>
<th>Total IT Load</th>
<th>Recommended Cooling System (Assumes Chilled Water Access)</th>
<th>Alternative Cooling System (Assumes no Chilled Water)</th>
</tr>
</thead>
</table>
| 0 – 20 kW     | 1) EF  
2) AHUOSA  
3) FCU | 1) HA  
2) SAC  
3) CRAC |
| > 20 kW       | 1) AHUOSA  
2) CRAH  
3) FCU | 1) HA  
2) SAC  
3) CRAC |

Key to abbreviations:

HA = House air

AHUOSA = Chilled water AHU with outside air economizer

FCU = Chilled water fan coil unit

SAC = Split DX AC system

CRAH = Chilled water computer room air handler

CRAC = Computer room air conditioner

EF = Exhaust fan with undercut door/louver

A centralized environmental monitoring system shall be installed and extended to each of the types of rooms. An appropriate temperature and humidity set point shall be identified for each room type, and the corresponding rooms shall be monitored and alert on temperature and humidity level changes. Floor sensors shall also be installed in each room to alert if there is water on the floor of the room.

Access Control

Due to the sensitive nature of the equipment installed, room security and access control are critical. Access controls provide the ability to not only control access, but to also potentially record and track who access the rooms and at what times.

All Equipment Rooms and Entrance Facilities shall have a windowless, solid core, door installed with the locks cored with a campus standard key system. In addition, an electronic card access or biometric readers shall be installed providing access to authorized staff and contractors.

All Telecommunication Rooms shall have a windowless, solid core, door installed with the locks cored with a campus standard key system. In addition, an optional electronic card access or biometric readers shall be installed as deemed necessary.

Infrastructure support

Certifications

All work associated with Entrance Facility (EF), Telecommunications Room (TR) rooms, and cabling/fiber shall comply with the National Electrical Code, state and local building codes. The guidelines developed by ANSI/TIA/EIA/UL and BICSI shall be followed in both design and installation.

The installation of all low voltage cabling and fiber shall be completed by licensed contractors and include end-to-end solution certification (Hubbell/Leviton).

Standards

All EF rooms shall be connected to the campus fiber backbone utilizing a minimum of a 24 strand singlemode OSP fiber, with a 600 pound tensile strength.

Each TR shall be connected to the EF utilizing a minimum of a 12 strand singlemode tight buffered 900 micron OFNP fiber.
Each endpoint outlet shall be connected to the TR/EF utilizing a minimum of a 23 AWG Cat6 cabling. Each Access Point location shall be connected to the TR/EF utilizing a minimum of a 22/23 AWG Cat6A copper cabling. To support Centrex lines, a minimum of a 4 pair Cat5 cable shall be pulled to each EF/TR. All copper cabling shall be CMP or CMR cabling, based on local codes.

To facilitate the proper installation, routing and placement of cables, the TR’s shall be located to assure compliance with TIA/EIA distance limitations. The total distance of the cable path between the telecommunication outlet and its termination in the TR shall not be more than 90 meters (295’).

Cable Trays - A ladder style continuous run of at least 10” wide and 4” deep of aluminum cable tray (unless specified otherwise in project design) shall be used in all drop tile corridor spaces. 4”Dx6”W outboard rungs will be installed on an accessible side of the cable tray for the purpose of supporting low-voltage cabling not affiliated with IT networking infrastructure (such as HVAC, card access, security and fire alarm cabling).

Cable tray shall be installed in a way that is reasonably accessible from drop tile corridors and at a range of 6” to 24” above the ceiling. Cable tray shall enter the EF/TR at a height as low as possible or no higher than 2’ above the corridor ceiling. Cable tray shall be accessible for a majority of the run with a 6” minimum clearance on both at least one side of the cable tray and below the cable tray.

The tray should stub into all EF and TR rooms, no further than 6”, via a rectangular slot that is sized appropriately to the cable tray. The only accepted cable tray is Cooper B-Line Redi Rail with 9” ladder spacing. Basket tray will only be accepted as a support system upon IT approval. Typically approval of basket tray use will be in open ceiling environments.

Riser and Horizontal Cable Pathways - Riser or distribution cables entering/exiting the TR shall be via two (2) 4” conduits or sleeved cores. The conduits shall penetrate the floor at a range of 3” to 6” AFF and shall be capped with a plastic bushing. Riser conduits shall stub down from the ceiling at a range of 8.5’ to 10’ AFF to allow for ease of access for installation and firestopping.

Horizontal cable pathways into rooms shall be a least one (1) 2” EMT conduit sleeve capped on both ends with a plastic bushing. Additional sleeves may be specified during project design to accomodate the amount of cables.

The use of J-hooks as the main horizontal pathway will be discouraged. Minimum standards require that J-hook routes are not more than five (5) feet apart. J-hooks shall be accessible with a minimum clearance of six (6) inches above and below. J-hooks shall be independently supported if possible to threaded rod or attached to the wall.

Data Network Design

IP Addressing

IP addresses are critical in placing phone calls over the internet. To send data from the right caller to the right recipient, the VoIP service needs visibility of the IP addresses of the devices involved.

IPv4 only provides approximately 4.3 billion IP addresses. As the number of end users and end devices continues to increase, IPv4 is reaching its upper limit and will soon be unable to provide new addresses. IPv6 provides significantly more IP addresses, as a result IPv4 will eventually be phased out in favor of IPv6. Most devices are already capable of handling IPv6 addresses.

IPv4 addresses are written as a string of four groups of numbers between 0 and 255, which are separated by dots, for example 192.168.0.1. IPv6 addresses are considerably longer strings of numbers, so they are written using hexadecimals. In addition to the 10 digits 0-9, six letters are added a-f. This means that each digit can have 16 different values, which results in more combinations. An IPv6 address has 8 groups of four hexadecimals separated by colons rather than dots, for example 2001:0db8:0000:0000:0000:0000:0000:0053. To simplify IPv6 addresses, if two colons are together it means only 0s are contained between them. For the previous example, it could also be written as, 2001:0db8::53.

It is recommended to allocate contiguous IP address space for IP phones and devices. It is also recommended to use 802.1Q user trunking or separate phone and data connections to the switch, as well to utilize non internet routable IP addresses as a security precaution for IP phones.

Multicast Music on Hold (MoH) audio sources should be configured to use IP addresses in the range 239.1.1.1 to 239.255.255.255, which is reserved for administratively controlled applications on private networks.

Power over Ethernet (PoE)

Power over Ethernet (PoE) is a technology that allows devices to be powered with an Ethernet cable, instead of an A/C adapter. There are two types of Power over Ethernet: PoE and PoE+. PoE is the standard version, delivering up to 15.4 watts of power which supports most VoIP phones. PoE+ is a newer version, delivering up to 25.5 watts of power. Benefits of using PoE/PoE+ include:

- Eliminate the need for separate power and data cables
- Ability to install PoE/PoE+ devices anywhere, without a power outlet, as long as the ethernet cable is within 300 feet of the switch
- Save on installation, maintenance, and energy costs
- Enable power-saving and on/off controls from remote devices
- Easier to perform remote power cycling
- Easier to perform diagnostics and status reporting on device power usage
PoE+ devices can also be connected to standard PoE switches. When this happens, the PoE+ device will restrict how much power it uses accordingly, but will still receive PoE level power. Similarly, PoE devices can be powered by PoE+ switches. A minimum of 1G PoE capable switches should be installed to support IP phones. If the environment includes higher powered capable devices, for example the latest generation of Access Points, the recommendation is to utilize PoE+ switches for all devices, including IP phones, to more efficiently utilize PoE capable switch ports.

DNS

Domain Name Services (DNS) is a critical network naming service. Network clients and servers both request connections to other devices by specifying a name. To resolve the name to IP address a request is sent to a configured DNS server and from this point on the client can use the returned IP address. DNS servers should be located centrally within core areas of the network with backup servers available. DNS should also be set up as a hierarchy with a master and secondary so the secondary servers are updated in an appropriate time frame. Devices should also be named and routers should have DNS entries for all ports to avoid IP address conflicts. Network devices should also be set up with backup DNS servers in case the primary server is down.

To aid in the overall management, it is recommended that all network devices & telephony related devices be added to DNS using a standard network naming convention that identifies the device type, device location and unique identifier for the individual device.

DHCP

Dynamic Host Configuration Protocol (DHCP) is used for client IP addressing, allowing for mobility and improved IP address manageability. DHCP servers shall be configured in redundant pairs, allowing for failover in the event of a failure. In addition, a recovery plan should be developed in the event of a DHCP service failure. DHCP servers should also support option 150 for IP phone provisioning. This permits the DHCP server to pass control to the Unified Communications Manager to download phone configurations following IP address allocation.

NTP

Network Time Protocol (NTP) allows network devices to synchronize their clocks to a network time server or network capable clock. NTP is critical for ensuring that all devices in a network have the same time. When trouble shooting or managing a telephony network, it is crucial to synchronize the time stamps within all error and security logs, traces, and system reports on devices throughout the network.

This synchronization enables administrators to recreate network activities and behaviors based on a common timeline. Billing records and call detail records (CDRs) also require accurately synchronized time.

QoS

Voice quality is affected by two major factors, lost packets and delayed packets. Packet loss causes voice clipping and skips. Packet delay can cause either voice quality degradation due to the end-to-end voice latency or packet loss if the delay is variable. If the delay is variable, such as queue delay in bursty data environments, there is a risk of jitter buffer overruns at the receiving end. To provide consistent voice latency and minimal packet loss, Quality of Service (QoS) is normally needed (except in cases where bandwidth is always available). The following major rules apply to QoS in campus environments:

- Use 802.1Q/p connections for the IP phones and use the auxiliary VLAN for voice
- Classify voice RTP streams as EF or IP precedence 5 and place them into a second queue (preferably a priority queue) on all network elements
- Classify voice control traffic as AF31 or IP precedence 3 and place it into a second queue on all network elements
- Enable QoS within the campus if LAN buffers are reaching 100% utilization
- Always provision the WAN properly allowing 25% of the bandwidth for overhead including routing protocols, network management and Layer 2 link information
- Use Low Latency Queueing (LLQ) on all WAN interfaces
- Use Link Fragmentation & Interleaving (LFI) techniques for all link speeds below 768 kbps

It is critical to enable QoS globally. When QoS is globally disabled all frames/packets are passed through switches unaltered which is equivalent to a trust CoS and trust DSCP state on all ports. In addition, when QoS is disabled, voice bearer and control traffic will not be prioritized and receive preferential treatment during network congestion.

LLDP/CDP

In 1994, Cisco introduced the Cisco Discovery Protocol (CDP) to provide the ability to automatically discover devices, and device information, connected to the network. As additional services, such as voice, became dependent on discovery capabilities, interoperability problems between vendors became problematic. As a result, the Internet and IEEE community developed the Link Layer Discovery Protocol (LLDP). LLDP was subsequently enhanced to specifically address the voice application, creating the extension called LLDP for Media Endpoint Devices (LLDP-MED).

Device discovery capabilities which are essential for voice services include:

- Capabilities Discovery - to determine the type of capabilities the connected device supports. It can be used to indicate whether the connected device is a phone, a switch, a repeater, etc.
- Network Policy Discovery - provides a mechanism for a switch to notify a phone the VLAN number that it should use. The phone can plug into any switch and obtain its VLAN number.
- Location Identification Discovery - allows a phone to be aware of its location information that can be used for location based applications on the phone. More importantly, this capability can be used to provide location information when making emergency calls.
- Power Discovery - allows switches and phones to convey power information, which is an especially important capability with PoE.
- Inventory Discovery - provides a means to effectively manage assets related to phones, as it allows a phone to inform the switch about attributes of the phone such as model number, serial number, and software revision.

Telemanagement Systems

Telemanagement system represents management of an organization’s telephone and telecommunications systems, which includes maintaining and ordering new equipment and monitoring expenses for usage

Service Tracking Tools

1. Services Tracking tools provide cradle to grave tracking of all inventory and assets. This includes, but not limited to, the following elements
   a. Invoices - include tracking of invoice vendor, account number, invoice number, PO number, amount payable, vendor contact information, contact information of department using the service, issue and due dates, and approvals queue if applicable
   b. Work orders and/or trouble tickets
   c. Provides quick management insight regarding work levels (orders and tickets) at different locations
   d. Tracks orders status and resource assigned to the order/ticket
   e. Automatically sends customer notification when order/ticket is resolved/updated
   f. Detailed integration with Service Desk for visibility into equipment and circuit histories

Inventory of circuits, instruments, and DID’s

1. Tracks and maintains inventory ‘bill of materials’ profile for all networking components—equipment, cards in that equipment, ports, etc.
2. Provides a catalog to quickly find any service, hardware, circuit, and network element (i.e., location, equipment, etc.)
3. Provides utilization and status (used/available/reserved) reports
4. Provides instruments assignment/types reports, i.e. which employee/department/service is assigned which phone (digital, analog, VoIP, and a license, including soft phones and voicemail
5. DID (Direct Inward Dialing) is the service provided by LEC

Cable management

1. The build/display cable path function is a tool that allows organizations to define all of the relevant components to build detailed cable paths from start to end so that you can easily track a path, including all of the relevant cross connection points. This way you can verify cable usage and capacity, automatically reserve cable paths as part of the Service Order process, and view cables by location so that you can proactively manage your cable plant rather than simply react to problems
2. Documents cable paths through all MDF, IDF including cable/pair number(s) and faceplate id’s. May include other cable/data network elements, such as network switch id and port number, speed/duplex, and any other tracked customized parameters
3. Provides visibility into rack configurations and component locations
4. Allows drill down from sites to buildings, rooms, and floors
5. View and maintain conduit configurations and access locations

Call Details Records

1. Call Detail Records is the detailed record of all the telephonic calls that pass through a telephone exchange or any other telecommunications equipment
   a. Reporting - The record is maintained by the telephone exchange and contains call details such as time of the call, duration of the call, source and destination number, completion status of the call, etc. Call detail records serve a valuable purpose of revenue generation for telephone service providers and are critical for law enforcement, whenever required. CDR is also used for VOIP and is a file containing all usage details such as source of origin and destination point of the call, usage period of the IP and the total amount charged during the billing period. Call Detail records are maintained by telephone exchanges emitting information in the form of tickets, with respect to individual customers/users
   b. Audit - provides a facility for configuring and importing CDR files from upstream telecom carriers. Once this call data is in the auditing tool, call margins and call exceptions can be identified
   c. The telecommunications industry is notoriously challenged by acquisitions, divestitures, legacy billing platforms, evolving technology, and cumbersome contracting and billing practices. These issues are detrimental to managing your telecom costs, all leading to billing errors and a loss of visibility and control. Keeping up with numerous contracts and lengthy, complex invoices can be challenging, or impossible, for many organizations. A regular and proactive audit of a company’s CDR will show services are off hook, and/or are not used over “x” period of time

Billing

1. When developing billing templates and configuring billing cycles, it is important to take into consideration CDR, departments and individual users identifiable information, IT Department service catalog, Carrier service catalog, and billing frequency
2. Billing tool not only serves as an ROI tool, but also helps make the right telecom spend decisions
3. Billing system allows telecom department to
   a. Reconcile billing with contracts, customer services records (CSRs), and internal data
   b. Validate services are billing in compliance with the appropriate contract, service order, or tariff filing and verify that surcharges are appropriate and calculated correctly
   c. Ensure telecom services that are being billed are being utilized
   d. Check whether wireless and wireline services and usage align with expectations, configuration information, and internal documentation
   e. Reduce costs by identifying opportunities to optimize the telecom services being purchased
   f. Establish policies to eliminate rogue spendings
g. Recover overpayments due to carrier and/or provider billing errors  
h. Identify legacy technologies that can be easily replaced with better and/or less costly alternatives  
i. Align telecom services with users, locations, department, and account codes

Monitoring/Metrics

SLA (Service Level Agreement(s))

ITIL focuses on three types of options for structuring SLA: Service-based, Customer-based, and Multi-level or Hierarchical SLAs.

A vendor signs a contract or Service Level Agreement (SLA) with a client to seal the deal. Before signing, carefully review the force majeure section of the contract as many carriers will use this to get out of providing credit for breached SLAs. The SLA contains the requirements and standards in which the operation of the contact center is based on. The Service Level KPI measures the organization's alignment with the goals and targets within the SLA.

Voice Carrier will make an initial response to service related incidents and/or requests submitted by the Customer within the following target response times examples:

Within 8 Business Hours for issues classified as High  
Within 2 Business Days for issues classified as Medium  
Within 5 Business Days for issues classified as Low

“Business Day” means regular business days in the USA, except U.S. public holidays  
“Business Hour” means between 6:00am to 5:00pm Pacific Time, Monday through Friday (Business Days only)

Target response time means the time by which Voice Carrier will first respond to a Customer’s support services request, but does not mean the time by which an incident will be resolved. This initial response may include questions seeking to clarify the incident or gather information on why the incident occurred and Voice Carrier may be unable to start resolving the incident before the additional requested information is provided by Customer.

Upon reporting the incident, Customer shall provide Voice Carrier with a complete and concise description of the incident, including all pertinent details and relevant hardware and software information. If Customer cannot provide information or data that reproduces the incident, Voice Carrier may be unable to solve the incident, but Voice Carrier will be available to work with Customer and use reasonable efforts to assist in the development of a test case that may be able to reproduce the incident.

In the course of analyzing an incident, Voice Carrier may identify a possible workaround. A “workaround” means an alternative method of using the Voice Carrier network which avoids the incident or minimizes its effect, which does not result in substantial extra inconvenience or expense for Customer, and does not result in any important reduction in the functionality of the Voice Carrier network. In that case, Customer will implement such workaround, and Voice Carrier may, at its sole option, modify the priority or the initial time limit accordingly.

Onsite assistance is provided only according to the terms of the Customer sales contract. Support for problems which were not caused by or within the responsibility of Voice Carrier may be available at the then current posted rates.

Some factors that may affect the Service Level include unplanned service outages, high call or ticket volume, and frequency of agent absenteeism. To ensure that a contact center meets the terms stipulated in the SLA, the above factors need to be addressed. In most outsourced inbound call centers, failing to hit the required service level can result in penalties and losing the contract.

The formula in calculating the Service Level might be different depending on the SLA and the contact center's preferences.

To calculate for the Service Level, divide the total number of calls answered within the threshold by the total number of calls and the total number of abandoned calls. Then multiply the result by one hundred.

Cloud Services

If a Cloud server hosting a Customer PBX or SIP trunk fails, another local server will typically be able to restore service within twenty minutes. In the event of the total failure of equipment in a colocation facility, or failure of a critical service required for ongoing operation which is provided by the colocation vendor (that makes service unavailable at the colocation facility), service will typically be restored on a separate system in a different geographical location within four hours.

Some products and services from third party vendors are licensed individually by those vendors. In the case of a system wide failure that results in a geographical failover, such products may not be available for use during the outage.

Some information, for example voice mail and call recordings, may not be available during a system outage that results in a geographical failover.

On Site Hardware

If any hardware at a Customer site which is provided by Voice Carrier fails, Voice Carrier will drop ship new equipment to the Customer within ten business days. Failed equipment is covered solely by any manufacturer warranty or the provisions of the Customer contract. Voice carriers may not stock replacement hardware. Voice Carrier may substitute different models of hardware or software, including those from a different manufacturer.

Voice Carrier will provide on-site support for system failures if separately contracted by Customer. For out of service or out of warranty equipment, Voice Carrier on-site support for installing any such equipment is available at the then current published rates.
Customer Provided Support

The Customer is responsible for providing support by Customer staff that Voice Carrier deems reasonably required in response to a system problem. Voice Carrier will not be able to repair certain system problems without the assistance of the Customer and Voice Carrier will not be held liable for any failure to perform under the terms of this agreement.

Customer is responsible for:

- First level triage of user incidents and service
- Basic replacement and configuration of defective desktop phone units and similar equipment
- Basic replacement and configuration of other hardware including a PBX, router, switch, bridge or gateway.
- Support and maintenance of phone accessories
- Coordination of incident resolutions of Customer owned data network service issues affecting system connectivity to WAN.
- First level user support for desktop phone feature operation and feature applications (e.g. explaining button layouts, basic feature operation, etc.)

Capacity Monitoring

Today’s commerce requires the interconnection of modern business communication systems with legacy voice networks. Demanding legacy requirements of a voice network can rapidly consume scarce capital and operational expense funds if not properly managed.

Leading practices suggest that effective network management include the following:

- Forecasting and Modeling - Typically the point of sale function within the enterprise provides an estimate of the business volume over time. Telephone service providers usually predict customer additions, disconnect and net volume over time. Standard customer behavior parameters (e.g. telephone usage frequency and average call duration) can then provide the basis to predict network capacities needed to meet the anticipated customer demand.
- Trending and Analyzing - Any model is strengthened with empirical field data. Actual customer usage should be monitored to refine the model thereby improving its ability to predict future needs. Any variations of significance need to be analyzed to determine if all samples are viable. In telephone networks, significant variations can be observed for high traffic days (e.g. Mothers Day, national disaster or radio/television calling campaign). These variations could artificially impact the desired long term engineering results.
- Augmenting and Optimizing - Reports and modeling provide insight into resource utilization. Any change, addition or reductions to the operating limit of the resource make require several days to accomplish in voice networks. Thus, it is important to model the augmentation process such that appropriate warning and alert levels can be established to provide the operator sufficient lead time to react to changing conditions. Leading operators define both low and high water marks for critical network resources to allow for additions when needed and right sizing of under utilized resources. The latter can have a large impact on recurring network expenditures.

Landline telephone users in the United States typically use between 500 and 750 minutes of call time monthly. Standard telephone engineering rules suggest that on average, 5 to 7.5 minutes of use per customer should be expected in the busy hour each day. The standard connection in the PSTN is a T1 which contains 24 separate voice channels. Traditional engineering guidelines for telephony suggest a T1 engineering capacity of 850 minutes of usage to achieve the PSTN standard grade of service of 0.5% call blocking. For demonstration purposes, each subscriber addition will demand 6.25 minutes of usage on that T1. Thus every 135 subscribers will necessitate an additional T1. In practice, the call minutes are typically spread across multiple connections based on specific communities of interest. The table below shows a typical growth scenario for our illustrative service provider.

The highlighted areas in the table indicate logical call groupings where augments are required to handle the growing telephony needs. If the above company is operating in 80 markets, then 300 subscribers will be added weekly in each market. It is imperative for the operator to have accurate forecasts for business growth so that trunk augmenting can scale in concert with the business. The techniques described in this paper are proven leading practices that simplify the role of the operator.

Capacity Management Simplified

Networks consist of resources working in concert to provide an end-to-end service offering. These network resources span customer premises equipment, access and transport nodes, inter-connection facilities and a backbone network. These elements are typically grouped into access, aggregation and core layers. Much of today’s voice traffic has migrated to wireless, cable, internet and other media while the traditional Public Switched Telephone Network (PSTN) provides legacy voice connectivity. Voice networks virtually transport packets of information from sender to receiver, and vice versa. The PSTN employs discrete packets of information at fixed time intervals. This technology, termed Time Division Multiplexed (TDM) traverses digital pipes throughout the PSTN over digital transport facilities. A T1 is a 1.544-Mbps transport typically configured as 24 separate voice channels and is the minimal connectivity between two nodes in the PSTN. A single T1 is capable of carrying 24 simultaneous TDM voice calls. The same T1 facility can be configured to carry significantly more calls using VoIP technologies that use various compression techniques and eliminate dedicated bandwidth consumption for periods of silence in normal telephone conversation.

Standard industry guidelines specify that a single T1 in the PSTN should be expected to carry about 850 minutes of call traffic or about 59% of the available minutes for a fully loaded T1. These minutes of usage (MOUs) include call establishment times, alerting, talking, disconnect and call tear down. A detailed explanation of the engineered T1 capacities is provided in Appendix I. For our purposes, this resource has an engineered limit as depicted in the figure below. As business scales and more call traffic is offered, it may become necessary to augment the transport with additional T1s. A second T1 elevates the engineered capacity of the transport to 2,050 available minutes of call traffic. There is a 20% efficiency improvement with the increased size of the pipe.

Trunk Group Alerting Levels - These alarms are designed to alert operations personnel when resource utilization reaches various severity levels of concern.

Increased Utilization
Unused Trunk Groups capacity is a cost that should be avoided. Right-sizing TGs in concert with market scaling can minimize these costs. In addition to daily fluctuations, voice traffic may have monthly, seasonal and holiday variances. The service provider needs to establish a busy hour and day as the basis. It is not necessary to attempt to engineer a voice network to handle all the calls offered on a holiday or in response to a calling campaign.

There are significant costs associated with unused trunk capacity. As noted in the example above, three TGs have a total of 18 T1s that are not planned to carry traffic in the sample study period. Each of these T1s has a monthly recurring cost of approximately $200 to $300 for a total monthly recurring cost of $3,600 to $5,400. These expenditures quickly scale when under utilization exists throughout the network.

Today, much of the traditional PSTN backbone has migrated to carrier grade IP-based networking. Voice providers are beginning to use their inter-connection LANs and WANs to carry on-net traffic and minimize the cost associated with handoffs to the traditional PSTN. The evolution will place more demand on the management of the voice application. It is imperative that networks be instrumented to provide application level insight for managing the voice GoS and the basic QoS as packets traverse multi-provider networks.

Monitoring Systems and H/W

Hardware monitoring software is designed to monitor the health and performance of your hardware assets. Failed hardware can lead to poor server performance or even worse system outages, this can cause downtime for critical business systems. At a glance hardware monitoring can help with the following:

- Identify server hardware health issues such as high temperature, bad disks or high CPU usage
- Provide alerting and notification of server and hardware issues
- Capacity planning and forecasting
- Minimize server and application downtime

Monitoring and management software usually includes:

Server and Application Monitor - this tool gives you the ability to monitor and inventory IT hardware and software assets. Monitors server CPU, memory, disk space, network utilization and more. This tool also provides basic monitoring of VMware and Hyper-V hosts and virtual machines.

Virtualization Manager - this tool provides in depth monitoring, performance management, capacity planning and optimization for virtual environments such as VMware, Hyper-V, and Nutanix. The tool should monitor virtual hard disks and allow admins to be alerted to disk space issues for zombie VMs, unneeded snapshots, and orphaned VMDK files. This can really help reclaim unused disk space.

Storage Resource Monitor - this tool provides a comprehensive view of the performance and capacity of your storage environments. This tool provides a single pan of glass into all your storage devices making it easy to view capacity and monitor performance. This tool can monitor just about any SAN, NAS or storage device including HP, EMC, NetApp, Pure Storage, Nimble and more.

Web Performance Monitor - this tool tracks user experience and tests web transactions for internal and external websites and web based applications. This tool will help you quickly identify slow or failing components down to the server, database or hardware level.

Please find a more detailed reference to top 10 monitoring and management tools here.

Monitoring Licenses

Administrators of telephony systems should be able to receive automated alerts about usage and capacity of issued licenses.

When the capacity usage approaches the licensing limits, notifications are to be sent to alert internal or external entities (such as partners). These notifications help administrator(s) determine the need to acquire additional capacity or reduce the scope of data to protect.

Most commonly, the following license related alerts are desired:

- Licenses consumed exceed n%  
- Licenses that will expire within n days

QoS (Quality of Service)

You can use the quality of service (QoS) monitor to analyze your IP traffic through the system. The QoS monitor helps to determine where congestion is occurring within your network. Quality of Service (QoS) is a method to prioritize network traffic going through a router to provide acceptable service to most users. Administrators put QoS in place to address audio quality issues. VoIP is susceptible to network congestion, resulting in echoes, lag, and dropped calls.

QoS (Quality of Service) is a major issue in VOIP implementations. The issue is how to guarantee that packet traffic for a voice or other media connection will not be delayed or dropped due to interference from other lower priority traffic.

Things to consider are:

- Latency: Delay for packet delivery
- Jitter: Variations in delay of packet delivery
- Packet loss: Too much traffic in the network causes the network to drop packets
- Burstiness of Loss and Jitter: Loss and Discards (due to jitter) tend to occur in bursts

Latency
Callers usually notice roundtrip voice delays of 250ms or more. ITU-T G.114 recommends a maximum of a 150 ms one-way latency. Since this includes the entire voice path, part of which may be on the public Internet, your own network should have transit latencies of considerably less than 150 ms.

Most network SLAs specify maximum latency

Axiowave SLA 65ms maximum latency
Internap SLA 45ms maximum latency
Qwest SLA 50ms maximum latency – Measured Actual for Oct 2004: 40.86ms
Verio SLA 55ms maximum latency

The SLA numbers above are for backbone providers, the total latency for a VOIP call may also include additional latency in the VOIP provider’s and the user’s local ISP networks.

Jitter - can be measured in several ways. There are jitter measurement calculations defined in:

IETF RFC 3550 RTP: A Transport Protocol for Real-Time Applications
IETF RFC 3611 RTP Control Protocol Extended Reports (RTCP XR)

But, equipment and network vendors often don’t detail exactly how they are calculating the values they report for measured jitter. Most VOIP endpoint devices (e.g. VOIP Phones and ATAs) have jitter buffers to compensate for network jitter. Quoting from Cisco:

Jitter buffers (used to compensate for varying delay) further add to the end-to-end delay, and are usually only effective on delay variations less than 100 ms. Jitter must, therefore, be minimized.

What’s an acceptable level of jitter in a network? Several network providers now specify maximum jitter in their SLAs.

Axiowave SLA 0.5ms maximum jitter
Internap SLA 0.5ms maximum jitter
Qwest SLA 2ms maximum jitter – Measured Actual for Oct 2004: 0.10ms
Verio SLA 0.5ms average, not to exceed 10ms maximum jitter more than 0.1% of time
Viteria SLA 1ms maximum jitter

The SLA numbers above are for backbone providers, the total jitter for a VOIP call may also include additional jitter in the VOIP provider’s and the user’s local ISP networks.

Packet Loss

VOIP is not tolerant of packet loss. Even 1% packet loss can “significantly degrade” a VOIP call using a G.711 codec and other more compressing codecs can tolerate even less packet loss.

The default G.729 codec requires packet loss far less than 1% to avoid audible errors. Ideally, there should be no packet loss for VoIP.

Most network SLAs specify maximum packet loss

Axiowave SLA 0% maximum packet loss
Internap SLA 0.3% maximum packet loss
Qwest SLA 0.5% maximum packet loss – Measured Actual for Oct 2004: 0.03%
Verio SLA 0.1% maximum packet loss

The SLA numbers above are for backbone providers, the total packet loss for a VOIP call may also include additional packet loss in the VOIP provider’s and the user’s local ISP networks.

Call Center Performance Metrics

Front-facing employees are the lifeblood of a business. Being in the frontlines, they brave through the challenges that come with delivering great customer experience on a daily basis. How does a contact center know it’s consistently delivering high quality service? It begins with setting metrics.

1. First Contact Resolution (FCR) - capacity to solve problems, answer questions, and provide needs the very first time a customer calls.
2. Cost Per Contact refers to the expenses related to running a contact center (i.e., operational costs, wages, benefits). To calculate the average cost per contact, the total cost associated with operating the business is divided by the total number of contacts handled.
3. Abandoned Call Rate (ACR) refers to the total number of calls where a caller hangs up before an agent answers. An inefficient IVR system may also cause callers to abandon the queue. To ensure compliance with the SLA, a 5% or lower abandoned call rate needs to be maintained. To compute the ACR, divide the total number of abandoned calls by the total number of inbound calls.
4. Average Speed of Answer (ASA) refers to the average amount of time wherein a call is required to be answered. It’s an essential part of the SLA where the service vendor promises to answer an X amount of calls within an X amount of time. Generally, a contact center’s ASA should not exceed 28 seconds. To calculate, divide the total amount of waiting time by the total number of calls received within a certain period. For
example, waiting for 20 calls while the total wait time is 30 minutes. The ASA in this instance is 1.5 minutes. The lower the ASA score, the less time customers spend waiting for their calls to get answered. A higher number indicates inefficiency and poor customer service.

5. Average Handle Time (AHT) is the average time spent by an agent in handling customer issues or transactions. This also includes the amount of time a customer is placed on hold within the duration of the call and the after-call work time which the agent spends doing back-office tasks. The AHT is calculated by adding the agent’s total talk time plus the total hold time plus the total after-call work time. This is then divided by the total number of calls. A low AHT isn’t always a good thing. For example, Agent A received a call from an irate customer. Frustrated and angry, the customer vents out. Agent A spent over 30 minutes on the phone but she was able to calm him while offering a win-win solution. Surely, Agent A’s AHT suffered but the interaction led to customer satisfaction and retention. On the other hand, Agent B received a call from another upset customer. Concerned that his AHT would suffer, he immediately gave in to the customer’s request to cancel his subscription. His AHT is exemplary but the client lost a great-paying customer. To improve AHT, quality training and customized coaching should be done. This should not only be limited to call handling and product knowledge, but should also extend to tool familiarity.

6. Average Call Transfer Rate is a metric that monitors the number of calls transferred to another department, a supervisor, or a different queue. To calculate, divide the total number of calls transferred by the number of calls handled and multiply it by one hundred.

7. Customer Satisfaction Score (CSat) is calculated by asking a question that pertains to the customer’s feedback on a particular interaction with an agent, “How pleased were you with your experience?” or “Was the agent able to handle your concern satisfactorily?” The customer is then provided with a survey scale where answers commonly range from 1 to 10, 1 to 5, or Very Satisfied-Satisfied-Not Satisfied. The highest number being the best and the lowest being the worst. Note that there isn’t any standard format currently observed but the scale hasn’t changed for decades. The agent’s Average CSat score is calculated by adding all of the scores received and dividing the total by the number of surveys received.

8. Customer Retention & Churn Rate. Customer Retention (CRR) and Customer Churn (CCR) rates go hand in hand. Retention rate refers to the percentage of existing customers or users that are still part of the organization’s pool of consumers within a certain period of time. To calculate the CRR, you would need the total number of active customers you have in a given period (30 days, 60 days, 360 days, etc.), and subtract the newly acquired customers during the same period. The result would be the total number of customers an organization has retained. For example, the number of customers you began with 2800 customers. During a 60-day period you acquired 300 more and ended with 2800. [(2800-300) / 2800] x 100 = 82% retention rate.

On the other hand, churn rate refers to the percentage of customers you have lost. This can be determined by dividing the number of customers who left by the number of customers you started with and multiply it by one hundred. For example, in a span of 30 days, the client has lost 150 customers while you started with 1,500. The formula would look like this: (150/1500) x 100 = 10% churn rate. These metrics determine whether an inbound contact center is capable enough to retain customers through providing excellent customer service. Generally a 5-7% churn rate annually is a healthy average. This means an organization’s monthly churn rate should only be .5% or lower.

Security and Compliance

Lifecycle and Access Control

The use of Access Control Lists to restrict incoming calls from remote endpoints is strongly recommended. Organizations should also perform frequent log analysis to see if unexpected incoming or outgoing calls are being made.

Many workers are now using their own headsets, earphones, webcams and other UC hardware, and while there’s nothing wrong with many BYO devices, a common problem is lack of integration and compatibility.

Consequently, IT teams need a clear, end-to-end picture of what is going on inside an organization’s entire communications infrastructure. Each device, or endpoint connecting to your network becomes a potential entry point into your IT infrastructure. With a high volume of data movement and applications interacting with these endpoints, institutions run the risk of security breaches. Endpoint monitoring tools should be set to automatically create alerts when a device is at risk.

The problem with some vendor monitoring tools is some of the devices in your network may be compatible, while others may not integrate well with your new platform. You may have devices that worked perfectly well until you introduced another platform, or one endpoint user may have added a new device which has not been configured correctly. This all leads to limited functionality and reduced productivity. A vendor agnostic monitoring and troubleshooting tool is the best option because they are more likely to find where the problems lie, and how to fix them.

HIPAA

HIPAA (Health Insurance Portability & Accountability Act) standards, which are designed to protect sensitive patient data, regulate how a covered entity can handle PHI. Covered telecom entities must have measures and policies in place to restrict access to PHI to only those with explicit permission.

If a third party does not access or retain PHI, they may be able to operation under the Conduit Exception Rule instead of signing a BAA. The rule rad as follows; Third parties that transmit PHI without retaining or accessing the information other than on a random or infrequent basis as necessary to perform the services provided can operate under the HIPAA Conduit Exception Rule. The network a hospital or healthcare system uses to power their phones and 911 access would also fall under the conduit exception. Telecommunications carriers are another example of a Conduit Exception. Telecommunications carriers frequently do not need to sign a BAA to provide customers who are covered entities with voice service, 911 access, or phone numbers.

HIPAA Compliance with old style FAX'es was always challenging since securing an analog fax transmission can only be done with encrypting fax machines, or encryption devices connected to the machines. These options are expensive, and to be useful, everyone must have compatible machines. Encryption only addresses the transmission of FAX’es, it does not solve the additional problems listed below:

- FAXes are often left on the FAX machine for some period of time after they arrive. This makes the sensitive information available to anyone walking by the machine.
- FAX machines often save copies of received FAX’es internally. This makes it possible for anyone with access to the FAX machine to print out additional copies of the sensitive material.
- FAX machines generally print the transmitted messages on paper. This paper, if not destroyed, could be placed in an insecure location.

Security and Compliance

Lifecycle and Access Control

The use of Access Control Lists to restrict incoming calls from remote endpoints is strongly recommended. Organizations should also perform frequent log analysis to see if unexpected incoming or outgoing calls are being made.

Many workers are now using their own headsets, earphones, webcams and other UC hardware, and while there’s nothing wrong with many BYO devices, a common problem is lack of integration and compatibility.

Consequently, IT teams need a clear, end-to-end picture of what is going on inside an organization’s entire communications infrastructure. Each device, or endpoint connecting to your network becomes a potential entry point into your IT infrastructure. With a high volume of data movement and applications interacting with these endpoints, institutions run the risk of security breaches. Endpoint monitoring tools should be set to automatically create alerts when a device is at risk.

The problem with some vendor monitoring tools is some of the devices in your network may be compatible, while others may not integrate well with your new platform. You may have devices that worked perfectly well until you introduced another platform, or one endpoint user may have added a new device which has not been configured correctly. This all leads to limited functionality and reduced productivity. A vendor agnostic monitoring and troubleshooting tool is the best option because they are more likely to find where the problems lie, and how to fix them.

HIPAA

HIPAA (Health Insurance Portability & Accountability Act) standards, which are designed to protect sensitive patient data, regulate how a covered entity can handle PHI. Covered telecom entities must have measures and policies in place to restrict access to PHI to only those with explicit permission.

If a third party does not access or retain PHI, they may be able to operation under the Conduit Exception Rule instead of signing a BAA. The rule rad as follows; Third parties that transmit PHI without retaining or accessing the information other than on a random or infrequent basis as necessary to perform the services provided can operate under the HIPAA Conduit Exception Rule. The network a hospital or healthcare system uses to power their phones and 911 access would also fall under the conduit exception. Telecommunications carriers are another example of a Conduit Exception. Telecommunications carriers frequently do not need to sign a BAA to provide customers who are covered entities with voice service, 911 access, or phone numbers.

HIPAA Compliance with old style FAX’es was always challenging since securing an analog fax transmission can only be done with encrypting fax machines, or encryption devices connected to the machines. These options are expensive, and to be useful, everyone must have compatible machines. Encryption only addresses the transmission of FAX’es, it does not solve the additional problems listed below:

- FAXes are often left on the FAX machine for some period of time after they arrive. This makes the sensitive information available to anyone walking by the machine.
- FAX machines often save copies of received FAX’es internally. This makes it possible for anyone with access to the FAX machine to print out additional copies of the sensitive material.
- FAX machines generally print the transmitted messages on paper. This paper, if not destroyed, could be placed in an insecure location.
It is for these reasons that traditional FAX’es are addressed by the Safeguards Principle; “Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.”

The best way to be truly HIPAA compliant is to not send FAX’es at all. However, institutional inertia may require that FAX’es continue to be sent. If this is the case, the following are some sensible policies to help make the best of a less than ideal situation:

- Do not send PHI over FAX unless it cannot be sent over other, more secure, channels like delivery by hand, and secure email, etc.
- Only send the PHI needed; do not send additional information.
- Always use a cover letter to prevent casual reading of the first page of the FAX.
- Use saved speed-dial numbers for common FAX recipients to prevent numbers being mis-dialed. Test these numbers periodically.
- For any new recipient, verify the FAX number with a test send of a facsimile before sending the actual protected health information.
- Develop policies on what to do if a FAX was sent to the wrong place. This can be a HIPAA breach.
- Configure your FAX machines to never save copies of sent or received FAX’es.
- Make sure that PHI FAX’es never remain on the FAX machine after receipt, and that they are promptly delivered to the intended recipient.
- Develop policies on the storage, copying, and disposal of PHI FAX’es.
- Locate your FAX machines in a secured room where only staff who are authorized to use ePHI that may be transmitted through that machine can access it.
- Use dedicated FAX machines for ePHI and keep it well separate and secured, compared to any other FAX machines in use.

As we stated above the best way to send a FAX is actually not send a FAX at all. Instead the best method for document transfer is to follow a scenario like this: (Either a service provider, or a properly set up cloud storage account could work in the scenario below.)

- You (the sender) access a recipient’s web site using a secure (SSL) connection. This would need to be a secure web service designed for this purpose, or maybe a HIPAA Compliant Cloud Storage.
- You login to and upload the materials to be “FAXed”
- You enter an email address and possibly a FAX number of the recipient.
- The pages that you are “FAXing” are encrypted and saved in a database at your FAX service provider.
- The “FAX” recipient gets an email or FAX notifying them that they have a “FAX” and that they need to go to a web site to “pick it up”.
- The recipient goes to the web site and downloads the “FAX” over a secure (SSL) web connection.

The method outlined above is more secure than a traditional FAX, but because it is not really “FAX’ing” it is also subject to stricter HIPAA guidelines. So there are two approaches to “securing” FAX’es in in the modern Unified Communications environment. You can either take advantage of existing regulations by maintaining the traditional FAX architecture in the UC world, or move to a more secure option that requires a higher level of compliance.

**RTP, Signaling, Encryption**

Real-time Transport Protocol (RTP) runs on top of UDP, and while UDP is a connectionless protocol that does not guarantee delivery of data packets between hosts, applying RTP provides services like timestamps or sequence numbers.

RTP itself does not provide any mechanism to ensure timely delivery of data or provide other quality of service guarantees; it does not even guarantee delivery of packets or prevent out-of-order delivery of packets. Indeed, RTP encapsulation is only seen at the end systems, it is not seen by intermediate routers. Routers do not distinguish between IP datagrams that carry RTP packets and IP datagrams that do not carry RTP.

So the application of RTP to UDP does not solve the voice and video transmission quality issues associated with UDP like dropped or out of sequence packets. Real-time Transport Protocol (RTP) allows only allows for a message which carries data from the source to a particular destination. However, in telecommunications we need other types of messages in a session. These messages can control the transmission and quality of data as well as also allow the recipients to send feedback to the source. Real-time Transport Control Protocol (RTCP) protocol designed for this purpose.

RTP is an integral part H.323 standard for real-time audio and video conferencing among end systems on the Internet. H.323 governs how end systems attached to the Internet communicate with telephones attached to ordinary circuit-switched telephone networks. In principle, if manufacturers of Internet telephony and video conferencing all conform to H.323, then all their products should be able to interoperate and should be able to communicate with ordinary telephones.

The overall point is that RTP, RTCP, and H.323 are all critical standards for modern telecommunications. A firm understanding of their application is required to adhere to any best practices’ standard.

**Telecom Security**

Today’s Unified Communication networks need to be secure. Especially, as the scope, variety, and complexity of current cybersecurity threats are increasing exponentially. With the increased role of cloud technologies, DNS and DDoS attacks are among the most common threats to modern telecommunications.

In general, almost half of all telecom companies were victims of DNS-based malware and most of those companies needed three or more days to apply a critical security patch. What this data is telling us is that most telecoms are not prepared for the latest cyber threats

Telecommunications providers are under fire from two sides. First, they face direct attacks from cybercriminals who want to breach their organization and network operations. The second being indirect attacks from those in pursuit of their subscribers. The top threats currently targeting each of these frontlines feature many classic attack scenarios, but with a new twist in terms of complexity or scale that place new demands on telecoms companies.

The following are some of the most common threats facing Telecommunications system.
DDoS (distributed denial of service) attacks remain a serious threat to telecoms providers around the world as attackers discover ever more ways of boosting the power and scale of attacks. The telecommunications sector is particularly vulnerable to DDoS attacks when you consider the amount and distribution of the packets they deliver. The seriousness of a DDoS attack cannot be underestimated. Direct attacks can reduce network capacity, degrade performance, increase traffic exchange costs, disrupt service availability, and even bring down internet access if ISPs are affected.

The core infrastructure of a telecommunications company is also a desirable target for cybercriminals, but gaining access is extremely difficult. However, once inside the core infrastructure, attackers can easily intercept calls and data, and control, track, and impersonate subscribers.

Unaddressed software vulnerabilities, attackers are still breaching telecoms and gaining access to vast quantities of valuable, personal data. In many cases, attackers are exploiting new or under-protected vulnerabilities in software.

Misconfiguration of the hardware used by the telecommunications industry is another vulnerability. Many times, that equipment carries configuration interfaces that can be accessed openly via HTTP, SSH, FTP, or telnet. Consequently, if the firewall is not configured correctly, the hardware in question becomes an easy target for unauthorized access.

The vulnerabilities described above, as well as vulnerable network devices, malicious insiders, and social engineering threats are all part of a large palette of risks to telecommunications providers, and those institutions that rely on their services.

Telecommunications is a critical infrastructure and needs to be protected accordingly. The threat landscape shows that vulnerabilities exist on many levels: hardware, software, and human, and those attacks can come from many directions. Telecom providers need to start regarding security as a process – one that encompasses threat prediction, prevention, detection, response, and investigation. A thorough examination of a Unified Communications provider's policies and preparedness regarding security threats should be a part of any best practices. A comprehensive, multi-layered security solution is a key component of this, but it is not enough on its own. It needs to be complemented by collaboration, employee education, and shared intelligence.

Accessibility Requirements

1. https://www.access-board.gov/ada/
   a. Official site for mandating ADA compliance
2. Visual, hearing, wheelchair, caption phones, etc.
   a. The different types of requirements that will mandate how you deploy and support telecommunications devices
3. Relay station
   b. For hearing impaired situations to allow an TTY. ADA compliant system for continuity
4. Signer
   a. A signer is a person who can communicate conversationally with people who are deaf or hard of hearing. An interpreter is a person who is not only bilingual but has also received specialized training and credentials to develop the skills and expertise needed to mediate meanings across languages and cultures
5. Accessibility https://www.ada-compliance.com/
   a. ADA compliance directory for reference

Unwanted Calls

Harassment investigations
   a. Required formal request from University Police Department to IT for ‘traps’ and Call Detail Record searches
   b. In some instances, divert calls to University Police Department to hopefully discourage live spammers

Spam/Robocalls
   a. Ignored at low volume
   b. At higher volume or in cases of harassment can temporarily block source Caller ID

Regulatory Developments (STIR/SHAKEN)

1. STIR - Secure Telephony Identity Revisited
   a. A protocol for providing calling party information within a digital signature.
   b. Focuses on end devices and allows for the digital signature to be produced and verified in numerous locations (source: https://www.redcom.com/stir-shaken-overview/)
2. SHAKEN – Secure Handling of Asserted Information Using Tokens
   a. Focuses on how STIR can be implemented within carrier networks. STIR emphasizes the end devices, whereas SHAKEN helps define the deployment ecosystem. (source: https://www.redcom.com/stir-shaken-overview/)

1. STIR/SHAKEN Legislation
   a. United States
Here are some of the main qualities to look for in a self-service portal from the administrator's perspective.

Administrator Functions

1. TRACED Act - Telephone Robocall Abuse Criminal Enforcement and Deterrence (signed into law 2019). Raises the fines the FCC is permitted to levy on robocallers and increases the statute of limitations for violations to three years.
2. The bill also creates an inter-agency task force to address the problem and encourage service providers to implement call authentication capabilities.
3. A key mandate from the bill is the requirement for carriers to collaborate with each other to implement call authentication technology with some evidence that STIR/SHAKEN may be the preferred approach.

2. STIR/SHAKEN Framework
   a. STIR/SHAKEN is a series of protocols and a governance framework that ensure caller ID has not been spoofed, in order to reduce the number of illegal robocalls. STIR/SHAKEN works by authenticating and verifying encrypted information used to attest to the accuracy of caller ID information. When a subscriber makes a call, an originating voice service provider ("OVSP") adds a unique header to the network-level message used to initiate a SIP call ("SIP INVITE"). The OVSP uses an authentication service to create this "Identity Header" containing encrypted identifying information as well as the location of the public key that can be used to decode this information. When the terminating voice service provider ("TVSP") receives the call, it sends the SIP INVITE with the identity header to a verification service, which uses the public key that corresponds uniquely to the OVSP's private key to decode the encrypted information and verify that it is consistent with the information sent without encryption in the SIP INVITE. The verification service then sends the results of the verification process—including whether the decoding process was successful and whether the encrypted information is consistent with the information sent without encryption—to the TVSP. 
   b. Source: CommLawGroup

3. STIR/SHAKEN Implementation Requirements
   a. The FCC imposes three requirements on VSPs in order to carry out its STIR/SHAKEN mandate.
   1. A VSP that originates a call that exclusively transits its own network must authenticate and verify the caller ID information consistent with the STIR/SHAKEN authentication framework.
   2. A VSP originating a call that will exchange with another voice service provider or intermediate provider must authenticate the caller ID information in accordance with the STIR/SHAKEN authentication framework and, to the extent technically feasible, transmit that caller ID information with authentication to the next provider in the call path.
   3. A VSP terminating a call with authenticated caller ID information it receives from another provider must verify that caller ID information in accordance with the STIR/SHAKEN authentication framework. 
   b. Source: CommLawGroup

Redundancy/business continuity/disaster recovery

1. Examples BCR (with Lumen), remote PBX
   a. Business continuity routing from Lumen for forwarding DID numbers to a specific connection before it terminates to the PBX (upgrades, outages, disaster planning)
2. Multiple carriers
   a. Having multiple carriers for failover or redundancy
3. PSTN just for critical services
   a. Public Service Telephone Network for routing of critical services in an outage – as in a local PRI can be used for overflow for Long distance in the event an LD carrier failed or could not terminate a connection
4. Multi-paths call routing, failover
   a. Designing for multiple connections for failover, disaster recovery for systems, carriers, entrance facilities are all good practices if they can be funded accordingly
5. Multiple power sources per system and external to services, Generators, Rectifiers, UPS systems
   a. Recommendation for generators for brownouts, black outs, with reliable UPS or rectifier with battery systems.

Self-Service Portals for Voice Systems

A VoIP self-service portal is a web-based platform that telecommunication providers can supply to their customers. It empowers system administrators and end users to manage their own service, so they can make service-impacting changes to their systems from their laptop or mobile device.

End User Functions

Here are some of the end user functionalities to look for in a VoIP self-service portal, the example is given based on a self-care portal as configured at University of Wisconsin.

1. Change telephone PIN, see Cisco VoIP - Changing your telephone PIN
2. Add/change call forwarding, see Cisco VoIP - Call forwarding in self care portal
3. Add/change speed dialing, see Cisco VoIP - Setting speed dials on your telephone in the Self Care Portal
4. Add/change ring settings, see Cisco VoIP - Change ring settings in Self Care Portal
5. Change voicemail notifications, see Cisco VoIP - Change voicemail notifications in Self Care Portal
6. Adding Phone Contacts to Your Personal Address Book, see Cisco VoIP - Personal directories for Cisco phone in the Self Care Portal
7. View your devices, see Cisco VoIP - View My Phones in the Self Care Portal

Administrator Functions

Here are some of the main qualities to look for in a self-service portal from the administrator's perspective.

1. Redundancy/business continuity/disaster recovery
   a. Recommendation for generators for brownouts, black outs, with reliable UPS or rectifier with battery systems.
2. Multiple carriers
   a. Having multiple carriers for failover or redundancy
3. PSTN just for critical services
   a. Public Service Telephone Network for routing of critical services in an outage – as in a local PRI can be used for overflow for Long distance in the event an LD carrier failed or could not terminate a connection
4. Multi-paths call routing, failover
   a. Designing for multiple connections for failover, disaster recovery for systems, carriers, entrance facilities are all good practices if they can be funded accordingly
5. Multiple power sources per system and external to services, Generators, Rectifiers, UPS systems
   a. Recommendation for generators for brownouts, black outs, with reliable UPS or rectifier with battery systems.

Self-Service Portals for Voice Systems

A VoIP self-service portal is a web-based platform that telecommunication providers can supply to their customers. It empowers system administrators and end users to manage their own service, so they can make service-impacting changes to their systems from their laptop or mobile device.

End User Functions

Here are some of the end user functionalities to look for in a VoIP self-service portal, the example is given based on a self-care portal as configured at University of Wisconsin.

1. Change telephone PIN, see Cisco VoIP - Changing your telephone PIN
2. Add/change call forwarding, see Cisco VoIP - Call forwarding in self care portal
3. Add/change speed dialing, see Cisco VoIP - Setting speed dials on your telephone in the Self Care Portal
4. Add/change ring settings, see Cisco VoIP - Change ring settings in Self Care Portal
5. Change voicemail notifications, see Cisco VoIP - Change voicemail notifications in Self Care Portal
6. Adding Phone Contacts to Your Personal Address Book, see Cisco VoIP - Personal directories for Cisco phone in the Self Care Portal
7. View your devices, see Cisco VoIP - View My Phones in the Self Care Portal

Administrator Functions

Here are some of the main qualities to look for in a self-service portal from the administrator's perspective.
1. Reporting capabilities: Administrator should be able to visualize your virtual SIP service through robust reporting capabilities. Make sure your portal of choice allows you to analyze your system and make plans based on real-time data. Portal allows you to pull reports on telephone number usage, toll-free traffic and concurrent trunk utilization. With greater insight into your busiest hours, you can properly plan for upcoming staffing needs based on recurring trends.

2. Security: control over user roles and permissions, i.e. admin, read-only, billing. ability to view any changes that have been made on your account. From a small change of a Caller ID change to the rerouting of an entire trunk group, you’ll be able to see what’s changed, by whom and when.

3. Safety measures: as related to NG911 - portal should have templates to create, modify, remove, or bulk update your E911 records.

4. Redundancy: Administrator should be able to easily identify a telephone number routing order by viewing routing sequences. Failover of the portal in case of primary portal outage should be seamless to all users.

5. Inventory Management: optional, administrators may use different tools for tracking phone numbers

6. User experience: make sure your portal has an updated, easy-to-navigate interface

Contact Center

IVR - interactive voice recording

1. An integrated and usually automated communications system that coordinates all telephone and electronic contacts between an organization and the public

2. Capability to front end an ACD system for departments and abilities to use callback functionality

ACD - automatic call distribution (agents, supervisors, wall board, statistics)

1. ACD is short for automatic call distribution. It is a telephony system that automatically receives incoming calls and distributes them to an available agent. Its purpose is to help inbound contact centers sort and manage large volumes of calls to avoid overwhelming the team

2. Abilities to use agents for call centers to take multiple calls by logging into a queue

3. Recorded message for customers to announce time in queue, time to answer, or call back functionalities

AA - auto attendant

1. Auto attendant (or automated attendant) is a term commonly used in telephony to describe a voice menu system that allows callers to be transferred to an extension without going through a telephone operator or receptionist. The auto attendant is also known as a digital receptionist

2. A system that allows caller to choose options to get to a department, dial by directory, or “0” for more efficient way of call routing

Recording systems

1. Premise or hosted recording systems, if required by “law” or customer service, agent reviewing

2. Harassing call retention

3. Announcing per “legal requirements” to the customer this is being done for training and or other purposes

4. Retention – how long to keep the recording based on the purpose

Backend systems CTI (computer telephony integration), data dip

Computer telephony integration, also called computer–telephony integration or CTI, is a common name for any technology that allows interactions on a telephone and a computer to be integrated or coordinated. The term is predominantly used to describe desktop-based interaction for helping users be more efficient, though it can also refer to server-based functionality such as automatic call routing. Common desktop functions provided by CTI applications include:

• Screen popping - Call information display of caller's number (ANI), number dialed (DNIS), and Screen pop on answer, with or without using calling line data. Generally this is used to search a business application for the caller's details.

• Dialing - Automatic dialing and computer-controlled dialing (power dial, preview dial, and predictive dial).

• Phone control - Includes call control (answer, hang up, hold, conference, etc.) and feature control (DND, call forwarding, etc.).

• Transfers - Coordinated phone and data transfers between two parties (i.e., pass on the Screen pop with the call.).

• Call center - Allows users to log in as a call center agent and control their agent state (Ready, Busy, Not ready, Break, etc.).

Some use cases for CTI features are as follows:

1. [https://www.tenfold.com/what-is/computer-telephony-integration](https://www.tenfold.com/what-is/computer-telephony-integration)

2. Can be used for lookup tables based on ANI (Automatic Number Identification) of the incoming call

Directory Assistance/Main Number Operator

1. Premise - 5 digit like calling

2. Dialing between stations – for “0” or operator number

3. Off net - 10 digit like calling unless SIP trunking connected for integration or routing, porting numbers

4. Dialing 411, 0+

5. Hybrid - on premise and off net - integration

6. Ability to have both on premise and off premise operator services

Types of Call Centers
1. Inbound call center. An inbound call center employs agents who receive calls from customers
2. Outbound call center. In an outbound call center, agents call potential or existing customers rather than receiving calls from them
3. Virtual call center https://www.genesys.com/glossary (definition terms of contact center)

Fax

Analog Fax Environment

Traditional fax machines present numerous problems for the modern remote/hybrid worker. Stand-alone fax machines and individual internet fax accounts lack a connection or synergy among various modern telecommunications tools. Today mobile and remote workers must have access to voicemail, fax, email, and all other company communications as if they are working in the office.

Many educational environments have legacy analog fax machines, especially in the more heavily regulated areas such as healthcare, Human Resources, and Admissions. When institutions make the decision to modernize their telecommunications to a fully digital Unified Communications system traditional analog services like faxing are sometimes overlooked. Institutions should consider two important factors when looking at secure fax messaging, security, and cost.

Security

Conventional faxing can be made to be secure, but in practice it often is not. The communication protocol used for faxing has remained unchanged over the past three or four decades and still operates on such antiquated processes that few IT departments give it much thought at all. Since analog networks are more or less separate from the data networks on campus and not connected to the internet, there is a belief that those networks are more “secure”.

However, institutions should be thinking about their faxing infrastructure because a legacy fax environment can create several gaps in secure messaging. Paper-based fax documents left sitting on an office fax machine or worse, multifunction printer, can create both a security and compliance risk for organizations. Further, the “images” stored on a fax machine representing the documents it has transmitted is also another vulnerability for an institution’s sensitive data because those fax machine hard drives are typically not secured.

Cost

The analog facilities required to maintain a reliable analog only network can be costly on many fronts. First, the charges for analog service, whether it be TDM (Time-Division Multiplexing) POTS service or even analog DIDs, is usually greater than the cost of similar SIP/VoIP services. Service providers are gradually discontinuing traditional copper TDM services. As the carriers’ copper TDM outside plant network deteriorates, it is simply being decommissioned since the carriers no longer want to invest money in an antiquated and regulated service.

This same problem extends to the campus infrastructure. Few institutions want to use their scarce funds to maintain old CAT 2 or 3 copper plants and RJ11 jacks across campus. Instead, those funds are better spent on more future ready CAT 5 and 6 cabling with RJ45 jacks as the de facto standard.

Media Gateways/Analog to IP converters

Media Gateways or ATAs (Analog Telephone Adapter) offer a relatively easy and inexpensive alternative to more disruptive and expensive equipment and networks.

A media gateway is a translation device that converts media streams between dissimilar telecommunications networks. Originally conceived to bridge legacy TDM based voice networks with next-generation Internet Protocol (IP) based voice networks, media gateways are now used to convert voice and multimedia sessions in a wide variety of enterprise and service provider applications.

The best use for Media Gateways/ATAs in today’s telecommunications environment is to extend the life of legacy TDM gear—legacy PBXs, analog phones and access equipment, and analog lines for elevator phones, alarm systems and fax machines—while gradually introducing IP-based technologies.

Fax over IP (FoIP) and Centralized fax Services

Fax messaging was designed to work over analog lines on circuit-switched networks, and at most institutions it has not successfully made the transition to packet-based networks. T.38 is a well-established protocol for sending faxes over a voice over an IP network in real time.
The T.38 protocol defines the transport of data, in this case a fax, between PSTN fax terminals through a fax gateway, between two Internet-aware fax terminals, or from a PSTN fax terminal through a fax gateway to an Internet-aware fax terminal. A T.38 stream is sometimes referred to as Fax over IP (FoIP). PSTN fax terminals traditionally use the T.38 protocol to send analog data. To exchange analog fax data with a PSTN terminal over the Internet, the T.38 protocol first converts analog data into digital data. The protocol then converts the data back to analog on the receiving end if the receiver is a PSTN fax terminal.

Most often T.38 uses UDP to avoid delays. However, T.38 can also use TCP and RTP as well depending on the service environment.

FoIP can help an institution address the cost problems associated with analog line deployment for fax messaging, but it does not really address the security issues associated with a legacy fax, since many of the security concerns surrounding the traditional analog fax machine still exist with FoIP solutions.

A Centralized Fax Service utilizing T.38 and UDP is a good alternative to maintaining physical fax machines. Centralized Fax Services enable individuals or groups to send and receive faxes without maintaining a physical fax machine. Rather than having faxes print out, faxes are sent or received using email or by accessing a web page. Faxes are displayed using the PDF format and can be retained for a predetermined length of time depending upon the compliance level required.

Centralized fax services seem to offer a solution that reduces the cost of the service, while improving overall security. Of course, this assumes that digital network security is configured to the best possible standard. Centralized fax services are also flexible. Users may communicate with the server in several ways, through either a local network or the Internet. In a big organization with heavy fax traffic, the computer hosting the fax server may be dedicated to that function alone. If that is the case, the computer itself may also be known as a fax server.

### E911 and Next Gen 911

[https://www.fcc.gov/general/9-1-1-and-e9-1-1-services](https://www.fcc.gov/general/9-1-1-and-e9-1-1-services)

1. Dispatchable location information - non softphone (database with University or external like Intrado 911 ANI format)
2. Next gen 2022 is softphone accuracy (application forced log in) - PBX system may need to be able to define softphone from hard phone type
4. The three-digit telephone number "9-1-1" has been designated as the "Universal Emergency Number," for citizens throughout the United States to request emergency assistance. It is intended as a nationwide telephone number and gives the public fast and easy access to a Public Safety Answering Point (PSAP)

### Internal versus external routing for PSAP

1. **Internal** - on premise 911 system with security (University Police) PSAP and NON PSAP approved
   a. Routing of calls internal to our institution (on premise police, for dispatching and dispatchable location – requirement of a database to import to the system
   b. Caveat is a cell phone call or centrex, POT will route to the city PSAP and will have to be transferred to the University Police
2. **External** - routing to city, county PSAP
   a. Routing of call external from your institution (city PSAP)
   b. Caveat is there could be a C911 for conferencing in the University for information purposes
3. **Next Gen 911 with texting**
   a. Next Gen 911 is still in deployment and development – most states, cities are still working on these deployments
4. Conference 911 (C911) - PSAP and security bridge connection
5. Email to security office or designee if 911 is called
6. Sending an email to an official person responsible for notification of a 911 call

### Ubiquitous cellular, wi-fi (Fixed-Mobile Convergence)

1. The anomalies of dialing 911 through a Wi-Fi connection can be problematic, cellular 911 call reverts to the cell tower, small cell transport. If there is no cell coverage and the use of the Wi-Fi connection is used there may be erroneous information provided to the PSAP

### Device/User Tracking applications (guardian or like, find me, follow me)

1. [https://www.raveguardian.com/](https://www.raveguardian.com/)
2. Similar like applications that allow a connection to “buddy” or police for tracking for life safety

### Emergency Devices

**Emergency Blue Light Phones**
Analog emergency phones have been around for quite some time going back to the 1980s when campus security was under scrutiny following the murder of Jeanne Clery. Despite the decline in emergency blue light phone usage and the increased usage of cell phones and life safety mobile applications, emergency blue light phones still serve very important life safety functions for campuses. They can deter crime, serve as a safety marketing tool for student enrollment, and parents, students, and visitors still expect to see them on campus.

Traditionally, emergency blue light phones infrastructure consisted of analog phone connections and in most cases power for the blue light. Recent times saw the introduction of VoIP and cellular infrastructure. All three technologies have their pros and cons.

**Analog Emergency Blue Light Phones**

Typically, analog emergency phones run over traditional plain old telephone lines and are usually fed with power for the Blue Light identifying the devices serving emergency purposes. Ideally they should be connected to generator power.

By the early 2020s, these devices are starting to show their age on college campuses. Over time, weather has caused rust, water damage, and decreased the quality of the devices. With newer technologies such as VoIP and Cellular, there are more options to replace them. However, there are still some benefits for analog phones over VoIP and Cellular.

- Cheaper installation
- Support for longer cable length for installation
- If no blue light, only POTS connection needs to be delivered

**VoIP Emergency Blue Light Phones**

With campuses moving their traditional PBX systems to VoIP, they are considering replacing emergency blue light analog with VoIP. There are challenges in doing this such as ensuring emergency power, handling long distances that may require fiber, and costs. Some benefits include.

- Leverage newer VoIP infrastructure
- Utilize existing networking tools to monitor these devices
- Use VoIP tools and reports to determine quality of service

**Cellular Emergency Blue Light Phones**

For those difficult places to run network or analog connectivity, Cellular emergency phones provide good options for life safety. Adding solar power to these towers means they can be placed virtually anywhere. Cost and cell coverage quality is the main consideration of whether this solution meets your requirements.

**Comparison Chart**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Analog Blue Light</th>
<th>VoIP Blue Light</th>
<th>Cellular</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation</td>
<td>Easy, cheaper installation, especially longer runs.</td>
<td>Can be more costly, especially long runs.</td>
<td>Easiest, most flexible for installation since they can be installed most anyone, especially if solar power is used</td>
</tr>
<tr>
<td>Reliability</td>
<td>Proven reliability, including during power outages</td>
<td>Special considerations need to be made for VoIP, power or PoE, connected to building generations</td>
<td>Cell quality can be an issue depending on location</td>
</tr>
</tbody>
</table>

**Monitoring Emergency Blue Light Phones**

Since these devices are used for life safety, campuses should develop processes to monitor the availability and quality of these phones. These phones need to work when there is an emergency, if they fail, it could result in harm or loss of life. Consideration for monitoring emergency includes:

- Routing inspections or tests of emergency phones. Typically, this is done by the IT or Police department. This can be time consuming and frequency is driven by results of testing and failure rates
- Some vendors provide tools to test and monitor emergency blue light phones
- If using VoIP emergency blue light phones, standard networking tools can provide some monitoring functionality
- Utilize CDR data from these phones to determine call quality, especially if performing monthly manually calling tests

**Considerations for locations**

Determining the locations and quantities of emergency phones can be a difficult task, departments such as IT, facilities, risk management, and the police should collaborate together to determine ideal locations for emergency blue light phones. Some best practices to consider:

- Remote locations where cell receptions are poor
- Crime prone locations
- Entrances to buildings that are in poor lit areas or less traffic
- While it may be cost effective to place them on buildings, ideal locations should be away from buildings so they are more visible and provide better coverage
- Ensure these devices are fed from buildings that have generator power
Other best practices

- Unless special requirements, don’t install a keypad and simply provide a red button that calls emergency services. Optional additional button for non-emergencies. Keypad is one more component that could fail and that you need to test regularly.
- Ensure that where these emergency phones are installed that they are with ADA Compliance. Consider the ability for those in wheelchairs to be able to access and reach the device.

Elevator Phones

Elevator phones should be treated with the same care as emergency blue light phones as they are used when the elevator stops functioning. While cell phones can be used for emergencies in those cases, there could be times when there are poor signals. With elevator phones, considerations need to be made for analog vs VoIP. It is highly recommended that you test your elevator phones in the same manner and schedule as you do for your emergency blue light phones.

Life Safety and Mass Notification Application

An important part of telecommunications, especially in college campuses, is the involvement with life safety and mass notification. Life safety and mass notification applications need to be simple, fast, and agile. They need to accommodate delivering notifications across multiple channels in seconds. Delivering 10k+ emails, 5k+ text messages, hundreds of voice calls, screen takeovers, website updates, and social media in seconds is not uncommon.

Channels of delivery

Institutions must carefully consider the channels of communications and when to use them. Some channels may be appropriate for general announcements to the campus whereas in certain cases, all channels will be used. Be careful not to bombard your users with unnecessary notifications as they will experience notification fatigue and could ignore that important alert. Channels to consider include:

- Email
- Text Messaging
- Mobile app push notifications
- Voice calling, including off-hook calling
- Social Media such as Facebook and Twitter
- RSS Feeds
- Website banner
- Desktop screen takeover
- Digital signage takeover

Features to consider

Beyond sending alerts, there are some other functionality and features that you should consider when selecting a service.

- Cloud hosted solution is preferable in case some event takes your campus networking and communications offline, the cloud service will be available to get the alerts out.
- Mobile Blue Light function to press a button to immediately contact the campus police or other emergency services.
- Virtual walkhome to allow campus dispatch, friends, or family virtually watch students progress to their destination.
- Direct chat with campus dispatch to report suspicious activity or request assistance.
- Campus maps with key safety locations such as life safety stations.
- Geofencing to provide alerts when approaching an area of concern or incident such as gas leak.
- Easy customization to brand, add content and links.

Cloud or Hybrid Hosted Voice Services

Why cloud hosted phone systems?

In general, Unified Communications systems are hosted Software as a Service (SaaS) solutions but voice services have been mostly on-premise, especially in the days of PBX systems. When colleges and universities migrated from PBX to VoIP, they tended to implement on-premise solutions for various reasons, greater flexibility in feature set, integrations with legacy equipment such as analog devices, skill sets, and business continuity. As more vendors offer voice services in the cloud, many are considering migrating to the cloud to reduce infrastructure costs, maintaining physical infrastructure, and more simplified approaches to administration of voice services.

Architecture and Design Considerations for Cloud Hosted Voice Services

Cloud-only Hosted

When it comes to cloud hosted solutions, careful consideration needs to be high availability and business continuity. Typically, end users or devices connect via the campus internet service providers (ISPs). At minimum, institutions will want to have multiple ISPs, hopefully coming from diverse locations on campus and regionally diverse.

While cloud hosted providers will talk about all the redundancy built into their cloud solutions, in the end institutions need to architect for failures. Assume the cloud provider or your connectivity to them will fail or be degraded, consider the following.
• How is my 911 service impacted?
• What departments, such as your Campus Police Dispatch center, do I absolutely need to maintain service to and how?
• How do I have incoming calls to the main campus number? Can those numbers be redirected quickly to a cell number at the carrier level?
• What happens to the Emergency Blue Light phones on campus?
• Contact center support?

Hybrid Approach

As discussed above in regards to planning for failure, institutions may choose a hybrid approach. Perhaps migrate general voice services for 90% of the campus but keep an on-premise footprint for critical services or analog services that don’t function well in the cloud.

With the hybrid approach, routing of calls needs to be thought out carefully. Do you route all calls to the cloud, which leads to redundancy concerns? Do you route on-premises to one PSTN and the cloud service to another which can add complexity but provide redundancy?

Generally, 911 service comes from a single provider. If you opt for the hybrid approach, you will need to ensure that your 911 provider supports both on-premise and cloud as not all do.

Support for analog devices

Analog devices can be challenging with cloud hosted solutions. Just like VoIP implementations, you will need to utilize analog gateway to support analog devices. Cloud hosted vendor support for the analog gateway varies and new equipment may be required.

Credits

Mark Reynolds, Associate Director IT Telecommunications, University of NM, Bicsi RCDD
Kon Skovorodin, Voice Infrastructure / Service Manager, Information Technology, University of Massachusetts Amherst
John Buysse, Sr. Director, University Network & Telephony Services, University of Notre Dame
Jim Monek, Director, Technology Infrastructure and Operations, Lehigh University
Ellen Rayz, AVCIT&CTO, CCSF
Julian Koh, Director, Telecommunications and Network Services, Northwestern University
Kevin Passarelli, IT Technical Project Manager, Information Technology, University of Massachusetts Amherst
Jill Richmond, Assistant Director Finance, Information Technology, University of Massachusetts Amherst