Introduction

In the City of Kearney, a Kearney Public Sector Telecommunications (KPST) group was formed to regularly meet and discuss the strategic direction of telecommunications services in the City of Kearney. This group's purpose was to provide a collective direction for public sector agencies in Kearney to better share resources and provide a unified voice to the telecommunications providers in the community. As a part of this process, discussions evolved related to the use of Voice Over Internet Protocol (VoIP) technology within the public sector entities. In order to better understand VoIP, this group initiated a pilot project in July of 2003. The goal of this project was to evaluate systems from various manufacturers and examine best practices and/or lessons learned. The KPST group wanted to examine first hand if VoIP was effective, efficient, and reliable. This project would also provide an opportunity to examine various manufacturers' systems and evaluate issues related to cost, features, and the system's ability to work seamlessly with other VoIP systems across the State.

The Environment

Kearney Nebraska is a community in central Nebraska, the county seat of Buffalo County located on the north bank of the Platte River, with a population of approximately 28,000 people. Situated in the south-central part of the state, Kearney is 186 miles west of Omaha, Nebraska and 361 miles east of Denver, Colorado. Kearney is the home to the University of Nebraska at Kearney; 9 public and 2 private elementary schools; 2 public middle schools; and one public and one private high school; Good Samaritan Hospital, (a 287-bed acute-care facility); County Government (employing 200+); City Government (employing 200+) and State Government agencies (employing 250+). The Kearney area economy has developed with a balance to include: manufacturing, medical services, agriculture, regional retail and wholesale, tourism and higher education. The majority of residents work in the trade, retail, wholesale and services areas, though several thousand are employed in manufacturing and construction. Major employers include Baldwin Filters, Eaton Corporation, Coleman Powermate, Morris Press, Marshall Engines, West Company and Chief Industries Inc. The incumbent local exchange carrier (ILEC) in Kearney is Frontier, a Citizens Communications Company with corporate offices in Stamford, CT.

Why VoIP?

All of the literature promises VoIP as a feature rich, cost effective method of providing voice communications. The possibility that VoIP could save dollars on telecommunications services was worth exploring. Specific to the individuals in this pilot were the following facts:

- Many of the agencies involved covered several locations within the community and surrounding communities, with some agencies having locations in nearly every community in the State. These locations totaled approximately 40,000 telephone lines, and generate more than 3 million minutes of toll usage monthly. In many cases these locations are linked to a common WAN (Wide Area Network). The concept that toll calls could be made from one office to another

while bypassing the Public Switched Telephone Network (PSTN) and the fees associated with the PSTN was appealing.

- The agencies and departments involved in the pilot routinely move offices from one location to another. Often these moves require the addition of wiring infrastructure to meet the demands for both data and voice communications. The ability to share a common wiring infrastructure between voice and data traffic appeared to hold another possibility for cost savings in terms of construction.
- The rising cost of local telephone service was an additional reason for the exploration of alternative means of voice communications. By installing VoIP systems, the number of PSTN connections could be drastically reduced as opposed to the current Centrex environment. The potential savings could be remarkable as long as the costs of deploying and maintaining a VoIP network did not outweigh the savings.
- The local Centrex contract nearing an end and the University of Nebraska at Kearney, as well as the State offices in Kearney, are now faced with a decision. Currently Frontier Communications, the local exchange carrier, holds the Centrex contract. They also own the campus telecommunications wiring at the University. Even if another carrier were to propose service at a lower rate than Frontier, there would still be an estimated $250,000 in cable plant construction to replace the Frontier owned wiring.

The Plan

As the group started to work on a plan to implement this pilot, provider participants were identified and invited to participate in numerous ways. Some of the KPST participants had already initiated dialogue with potential providers of VoIP equipment, others asked for suggestions from contacts they had in other user groups, one KPST participant was on the verge of implementing the technology in their setting, and many providers contacted the group after hearing of the project. In order for a provider to participate in the pilot, the provider was required to provide a large business size VoIP system and approximately 30 IPO telephone sets. The system provided must be E911 capable and able to interface with the PSTN using ISDN BRI trunks. Each system was provided by it's vendor at no cost to the Kearney Public Sector Telecommunications group for a period of 30 days. The T-1's and circuits used for the pilot project were ordered, installed by and paid for by the Kearney Public Sector Telecommunications group.

Providers who wished to participate in the pilot project were invited to give a one-hour presentation opportunity to introduce their company and product offering to the KPST group on July 23, 2003. The majority of the providers took advantage of this opportunity.

Each of the public entities participating in the pilot project designated a Team Leader and a support group from their organization assigned to working with one of the participating providers. Three hour one-on-one training sessions with each provider were scheduled from July 28 through August 13. This training was open to anyone that wished to attend and went into detail on system operation, software, features, and options of the individual

systems. Each KPST entity was given the opportunity to test three VoIP telephones from each provider.

The original target date for equipment to be installed and ready for testing was August 1, 2003. However, due to the tight timeline, installation of the T-1's and circuits was not completed until the second week of August. This pushed back the initial start date for testing and system implementation.

Testing would be twofold. Each public sector entity was given the ability to place calls on the system. Secondly, a systematic and ordered test would be performed on each provider's system to document performance. Each provider would be able to be present for the tests that were performed using their equipment. These tests were schedule for the first part of September. The vendors would be asked uniform questions about the particular equipment they had installed for the pilot project. The questions tested and/or verified their equipment and software capabilities. Finally, testing would be completed to observe call quality under various network conditions and scenarios.

The Players

The following is a list of entities that participated in the project as a part of the Kearney Public Sector Telecommunications group.

Buffalo County
City of Kearney
Educational Service Unit #10 (ESU10)
Good Samaritan Hospital
Nebraska Educational Telecommunications Commission (NETC)
State of Nebraska-Division of Communications
University of Nebraska at Kearney
University of Nebraska at Lincoln
University of Nebraska Central Administration

The Equipment

3COM	NBX 100
AVAYA	S-8700
Intertel	8660
Mitel	3300
Nortel	Succession 3.0 with BCM
Siemens	HiPath 3000 and 5000

The PSTN

Each IP system was connected to the PSTN via Intergrated Services Digital Network Primary Rate Interface (ISDN PRI) trunks. Unlike typical T1 trunks, ISDN trunks utilize our of band signaling, allowing for full 64k voice due to the use of out of band signaling. To save on costs, only the "D" channel and 2 "B" channels for each circuit were installed. Although standard voice trunks, or even two wire direct inward dial trunks could have been used, PRI was chosen to ensure that the actual station number

would be outpulsed as automatic number identifications (ANI) to the PSTN. Typically, a single ANI is outpulsed for every call for other types of T1 trunks. This was important for two reasons. First, with the actual ANI being outpulsed, the long distance carrier could send accurate billing detail with the actual originating telephone number rather than the ANI assigned to the T1 circuit or one of its trunks. Station Message Detail Recording (SMDR) could then be used for validation of toll carrier billing records. Even though the carrier billing records would accurately identify toll calls from their originating stations, the system SMDR would still be needed for accounting of toll calls that traverses the IP network. Second, since PRI service outpulses the actual station number to the 911 call center, dispatchers are able to more accurately pinpoint the address of the caller instead of the address associated with the particular trunk from which the 911 call was sent. E-911 will be discussed in further detail later in this document.

PRI trunks can also be configured for direct inward dial (DID) service. This allows each telephone set to have it's own unique telephone number regardless of the number of trunks assigned to the system. If necessary, hundreds of telephone sets can have a unique number identification when the actual ratio of trunks to extensions may only be 6:1. If standard analog trunks are used, the number of unique telephone numbers assigned are limited to the number of trunks installed on the system. By using standard trunks, telephone calls can be routed to particular sets one of three ways. First would be to assign a trunk to each telephone set. This allows calls to be accurately routed to their destination. This does not make very economical use of the telephone system as a separate trunk would need to be purchased for each telephone set. The second method would be to send all calls to an attendant. By sending calls to an actual attendant, much of the attendant's time would be devoted to answering and routing telephone calls, again not a very economical use of a high tech system. A third option would be to route calls to an automated attendant where the caller could then be routed to an extension within the system. The group believed that in an actual deployment of any of these systems, there would be a need for DID service. Therefore in the pilot all systems tested were configured in that manner with PRI.

On a mature VoIP network, the data network available would be used to transport voice traffic from system to system. Aside from toll bypass, this would also reduce the need for PSTN trunking. This would reduce the overall cost for local telephone service. However, even with the worlds most robust, and sophisticated VoIP network, the need for reliable PSTN connectivity still exists. PSTN trunks connect a private network with the outside world. PSTN trunking also serves as a backup in the event that IP routes are either out of service or full.

The Network

As this pilot was discussed and planned, it should be noted that the KPST participants were not supported by a common LAN or WAN. In order to connect between the participants in this pilot, three T1 circuits were installed by the local exchange company. These circuits connected the Buffalo County Court House, Good Samaritan Hospital, and the City of Kearney to a common WAN with the rest of the participants.

All Kearney agency circuits as well as the University of Nebraska Kearney LAN were connected to a CISCO 7206 at the UNK campus in Kearney. A DS3 connected the 7206 with the University of Nebraska Central Administration (CSN) network located at the University of Nebraska in Lincoln. Nebraska Educational Telecommunications (NET), the State, and UNL were connected to the Kearney agencies via high speed WAN connections through CSN. The University of Nebraska Computer Services Network (CSN) router (referred to as UNK7206) interface for the call managers connected to a Cisco Catalyst 5509 on a port with a secluded virtual LAN (VLAN). Secluded, for this purpose, means there was no network connectivity allowed to that VLAN; only devices directly attached to it would communicate within that VLAN. On the 5509 two additional ports were assigned to that VLAN. One was directly connected to an Enterasys Vertical Horizon switch which provided connectivity for the Nortel, Inter-Tel and Mitel systems. The other was a VLAN trunk to a Cisco Catalyst 5505. Numerous ports on the 5505 were used to attach the Avaya, Siemens and 3Com systems. The only connectivity outside of the isolated VLAN was CSN's 7206.

The general path for a phone anywhere on the UNK campus would be:
From phone → to the building's switch, → to the central 5509, → VLAN trunk to UNK7507 router, → to UNK traffic rate limiter, → to CSN7206, → UNK5509 private VLAN, → either 5505 or Vertical Horizon switch as appropriate, → call manager. The path for a phone in the pilot is the same as above, substituting building's switch with the 5505. The UNK rate limiter performed no prioritization on any of the VoIP traffic. It simply passed it as is, i.e. it did not rate limit it.

To UNK all these systems looked like devices on the Internet. Each vendor may or may not have supplied their own switch to attach their systems to the UNK equipment. Nortel, Mitel and 3Com provided their own switches, which in turn attached to the UNK gear. The phone test bed was various ports on the 5505 which were in the same VLAN as the Communications Center. This VLAN is part of UNK's internal network.

Configuration on the CSN 7206 located on UNK campus included setting up controllers and serial interfaces to support the three T1 connections listed above. Other changes included defining IP routes, and Border Gateway Protocol (BGP) network statements. BGP allows other neighbor routers know its IP routing tables.

There was no Quality of Service (QOS) initiated on the network, aside from the select test calls requiring it. The UNK router also had a short (3-5 lines) access list on all interfaces to block pings and port 135 in order to limit viruses. The Internet interface (going to call managers, CSN7206) had a 40-50 line inbound and 40-50 line outbound access list filtering various IP address, ports, etc. The following is a list of the various WAN connections involved and their bandwidth capacities.

- UNCSN network (6509-FW-Core6509) to NU7507: Gig
- NU7507 to CSN LS1010 at our border: 155 Mb.
- CSN LS1010 to CSN 7206 at UNK: 45Mb.
- UNK network: 100 Mb

- CSN 7206 @ UNK to UNK7500: 100Mb
- CSN 7206 @ UNK to Call Managers: 100 Mb; later moved to 10Mb
- CSN 7206 @ UNK to 2610 @ City of Kearney: T1
- CSN 7206 @ UNK to 2610 @ Buffalo County: T1
- CSN 7206 @ UNK to 2610 @ Good Samaritan: T1
- CSN 7206 @ UNK to ESU10: 10 Mb
- ESU10 to Kearney Public Schools: 10 Mb
- UNL to UNCSN Core6509: Gig
- NETV to UNL: 100 Mb
- State of Nebraska to UNCSN Core6509: 10 Mb

Installation

Installation was accomplished over approximately 3-1/2 weeks. Many of the issues that were uncovered dealt with communication issues. This was a large project with six different vendors all working to install their equipment within the same general timeframe. Getting everyone on the same page was a major goal. The KPST team continues to ponder whether this goal was difficult because of the size of the project or the complexity of the project. It was also difficult to know whether issues arose because the vendors were not prepared or the KPST participants were not prepared.

Facilitation was a large part of the project for the KPST members. Generally none of the vendors were totally self-sufficient when it came to installation. They all needed something. There were questions about test design, network configuration, extension configuration, etc. KPST participates could only answer the network questions related to their piece of the network. It would be difficult to describe what the vendors needed. There were practical items such as where to put their equipment, what to connect it to, where to place themselves, and directing them to the correct people for information.

Although each vendor prepared their equipment prior to arrival at the installation location, there was a considerable amount of work that still needed to be done once they arrived on site with their equipment. Most of the vendors had at least 2 people on site for about 1-1/2 weeks – with the majority bringing in 3-4 people for the first week. There appeared to be a general confusion about what addressing schemes should be used in what parts of the pilot, getting the PRI/DIDs straight, "what are you going to do in this test," and other "what do we have to do to make things work" issues. The different vendors were at different stages of preparation prior to arriving in Kearney. The KPST team had taken steps to assure that the information was given to the vendors in writing. There were some modifications that took different timeframes to float between each vendor, which may have been some cause for the time and resources needed to deploy the equipment. But the size and complexity of the project may have been the major contributing factor to the amount of time and resources that appeared to be necessary to get the project off the ground.

Because installation was done through a combination of both the user and the provider, information directly from the KPTS participants is most appropriate. The following represents comments from the user community related to the installation process. These

comments are perceptions of the users and not necessarily fact. However, it is important for the purpose of this test to understand the viewpoint of the actual users.

- I personally thought installation of equipment took a lot longer than it should have but then maybe my expectations were set too high. Some vendors seemed much more prepared than others. As a team I think we should have also been more prepared with documentation which might have helped the vendors more.
- The person who resides in that room where we did the testing could probably tell us a lot about what occurred behind the scenes in regards to the vendors who occupied that area. He had told me he overheard comments as they were setting up their equipment that they probably didn't intend on him hearing.
- The vendor displayed interest in establishing one-on-one help to each of the participants in the test. Phones were either pre-configured or time was spent instructing user how to configure their own. Gave out good documentation on the configuration of their setup. I received a manual with information about the products and whitepapers on VoIP. Also spent time with at least some of us going over the management of the Call Manager. Call Manager interface was "okay", just not as user-friendly as other ones. I used the softphone feature on my laptop. Worked fine once I used a USB headset instead of a normal headset using the PC sound card. The thing I didn't like about the softphone was that it took over the deskset instead of acting independently. Licensing feature using the softphone was set within the Call Manager software.
- The vendor pre-configured their phones but at least some of them were mis-configured most likely because they didn't have the correct IP information the first time around. Call Manager interface was easier to work with. Also used the softphone feature which used a physical device that plugged into a USB port. This provided the licensing feature. I actually preferred this softphone over others. Also required the use of the USB headset to get quality voice. On the this phone, my phone number was being handed out as a number for the Kearney Holiday Inn for registration. I had quite a few phone calls asking for information or to register. The vendor also gave out a CD with information on their product.
- This phone on my desk never did work. I believe that was reported to the vendor but it was never resolved. Never had any contact with this vendor.
- The individual techs with this vendor were very helpful each time I talked with them. Phones were pre-configured so when I went to re-configure them for the test in another location I had to get information on how to enter configuration mode. No manuals/documentation were included with the phones. The vendors was willing to let us continue to test with their equipment for another 3 weeks so that key people could test them.
- We were asked to test their wireless phone with our Cisco Aironet access point. When it did not work, the blame was put on the software of the Aironet which is not IOS. Said we would have to upgrade our software.
- I noticed one vendor had repeated problems with their servers which had to be rebooted to recover.

- My telephone came pre-configured but if I remember correctly had a configuration error. Was easy enough to fix once you figured out how to get into setup mode. Never had any contact with this vendor.
- Phone came pre-configured. Don't remember having problems with it but don't necessarily remember receiving phone calls on it. I believe I placed some but did not get any responses to voicemail.
- I had delusions of sitting by each vendor and picking their brains as to what they were doing. I did not have the time. There were so many **ordinary** mundane things they needed constantly, it is hard to even think of what took so much time. Generally I spent 6-10 hours a day "facilitating" for 3 weeks.

Blaster, Sobig and Welchia Worms

August 2003 was the height of several worm infections in the world. Although unplanned, this was an opportunity to see how the various systems reacted when an unplanned virus entered the network.

The Sobig worm is an email based worm initially released in January 2003, but had later updated versions on the Internet found. The most dangerous versions were released in June 2003. According to the McAfee website, when the virus successfully infects a Microsoft Windows based machine, it uses its own internal SMTP engine to mail itself to any email addresses found on the infected machine. This has the effect of creating thousands of new, very active mail servers on the Internet. Existing mail gateways are saturated with new messages that contain the virus attachments and in the case of networks that use Outlook and Exchange as their email providers the network and routers were saturated with traffic. In cases where Outlook was patched to the latest Microsoft standards user intervention was required to open the virus and continue the spread of Sobig.

Blaster was a different from Sobig in that it didn't use email or require user intervention to spread. Information on the McAfee web site related to Blaster stated, "an infected machine (running msblast.exe) will send out malformed packets across the local subnet to the RPC service running on port 135. When these packets are received by any unpatched system, it creates a buffer overflow crashing the RPC service on that system. All this can occur without the worm actually being on the machine. The remote shell still gets created on TCP port 4444, and the system may unexpectedly crash upon receiving malformed exploit code." This worm allows complete remote control of an infected machine and saturates the network with the infection attempts on port 135. Only Windows NT, 2000, and XP machines were effected by this worm.

The final worm to hit the Internet was the Welchia worm. This one came after Blaster was introduced. Its creator meant for it to clean up any Blaster infections automatically by exploiting the same vulnerability as Blaster. It however used a different method of finding machines to infect than doing a simple service sweep for port 135. Welchia sent out repeated ping sweeps (especially on the local network) looking for possible machines to infect. This increased the ICMP traffic to new unheard of heights, and brought routers

to 100% CPU utilization. This slowed down or completely disabled many large networks around the world.

The University of Nebraska Kearney network had an access list on the network to block ICMP pings or UDP traffic on port 135. The phones/PCs used in testing at the State of Nebraska, University CSN, UNL, and NET were all located behind firewalls. It does not appear that viruses bothered the telephone test bed much. At Kearney viruses were contained within buildings, and there were no viruses detected in the Communications Center in the test bed (lab). However, the call managers were in the open Internet in terms of the attachment to the UNK network. Unless there was something at UNL or CSN blocking viruses, the call managers were free and open "in the wild." One vendor's system appeared to become infected by Blaster. Other vendors had minor virus issues. Some of the personal laptops became infected; but they were being used for their own work needs. After receiving a phone call from University CSN Networking stating that it was flooding the network, the vendor was asked to remove it from the network. Their laptops had no real use associated with the VoIP test.

There was an occurrence on a server that was handling voicemail. When the virus ran, it infected the host computer and then emailed itself, using its own SMTP engine, to harvested email addresses from the email machine. As it propagated, the worm "spoofed" the "from: field", using one of the email addresses it had harvested With the ability to send so many emails, Sobig can really sap bandwidth and slow down network performance. The first two occurrences happened in early August before actual testing began.

Although the So-Big virus did not reveal any issues related to virus infection at the telephone level, the stress testing did show that the phones may be very susceptible to Denial of Service issues. In test performed using SolarWinds, results showed minimal traffic needed to be addressed directly to a telephone set to cause problems. Quality of Service (QoS) does not appear that it would not resolve this problem. QoS would prioritize VoIP traffic to the telephone, but the phone would still be flooded with DOS/DDOS traffic.

Security concerns

While it's easy enough for someone to pick up a standard Time Division Multiplexing (TDM) telephone and make fraudulent calls, it is still somewhat controllable from a physical security standpoint. However, it is far more difficult to control a situation where someone could make calls using a telephone number yet be physically located anywhere on the network or even the internet. One of the advantages VoIP vendors market with this technology is mobility. With many of the systems tested, users can move from one telephone set to another by merely "logging in" to the telephone by entering an extension number and a password that is validated by the system. This feature could require a whole new set of security policies surrounding personal telephone passwords. Furthermore, if someone fails to log out of a telephone set and another user begins to make calls, it would be difficult to hold anyone accountable for calls or ensure proper

billing for toll charges. This can create issues if calls are being accounted for and tracked.

Wireless access points are another security item worth mentioning. On one occasion a vendor probed the lab network for an open wireless access point and was able to gain access. Calls were placed using a laptop softphone while sitting in the parking lot. This opens security concerns beyond the issues that come with full integrated data networks, but opens the possibility for someone to gain access to the telephone system by wireless means. Even if the MAC (media access control) address is used to control access at the datalink layer on a network, this address can easily be spoofed by an attacker to gain access.

During the setup process the Cisco Pix firewall fixup modules did not work with some of the vendor telephones. The fixup modules enables the H323 protocols through dynamically as calls are made, limiting the opening of the entire IP range to the outside gateways or outside telephone sets. After opening up the firewall entirely from the Kearney gateways and removing the H323 fixups, the telephones worked. This indicates that there is some type of proprietary protocol that creates this incompatibility and may present a security risk if this is the only method to intermediate firewalls between the telephones and gateways.

Only one vendor indicated that encryption was built into their voice system. However, this was again due to a proprietary protocol that would not encrypt the data if it was sent to a different gateway.

None of the telephone piloted supported Ipv6 (which includes extensions for NAT and VPN). NAT is network address translation, which is commonly used to gain more IP address space for internal network use and security behind firewalls. VPN is virtual private networking, and is used to encrypt and tunnel local network traffic over unsecured network links. All vendors indicated that the telephones will be getting an update for IPv6, but none of the models has specific chips that are used to do encryption co-processing. Without these chips, if there is a need in the future for new encryption (which IPv6 is supposed to include) that uses more processing, it may not be possible to put on the telephone sets.

Most of the telephones piloted supported using a computer on the same data port, with separation done at the phone for the different vLANs. Software selection of vLANs assists with the management of traffic, but is easily attacked compared to hard setting the vLANs for the ports at the switch. A better solution appears to be a separate port for each telephone and computer, or to put the telephones on a different data switch entirely.

A technical test of the security of each system was done using two tools. Network Mapper (Nmap) was used for port scanning and Nessus for security vulnerability scanning.

Nmap is a free open source utility for network exploration or security auditing. It was designed to rapidly scan large networks. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap runs on most types of computers and both console and graphical versions are available. *(Taken from Security.Org's Web site at http://www.insecure.org/nmap/)*

The Nessus is a remote security scanner. A security scanner is a software which will audit remotely a given network and determine whether bad guys may break into it, or misuse it in some way. It will not consider that a given service is running on a fixed port - that is, if you run your web server on port 1234, Nessus will detect it and test its security. It will not make its security tests regarding the version number of the remote services, but will really attempt to exploit the vulnerability. *(Taken from Nessus.org's Web site at http://www.nessus.org/intro.html).* Just the act of scanning a service may crash the remote operating system in some cases.

The following represents findings made on the various vendors products:

- VENDOR 1: This vendor's telephone was picked up on the network with an open SNMP port. The service responded with a guessable community string, so data could be read from the telephone's status. According to the telephone engineer the only data that could be read was the status, but said that the functionally of the SNMP is being expanded at the request of another customer. The capability to disable this should be available as SNMP causes network congestion and is very insecure compared to alternatives. The administration interface of these telephones was to a control screen was via a telnet-like session. There was no encryption with the version of the control program. Information related to back up of the configuration conflicted between engineers and training instructors.
- VENDOR 2: This vendor's telephone was picked up with three main issues on the network. It also had the SNMP service open with a public community string. Another found service was a web service to do remote configuration of the phone. This is a problem due to the fact that the more a device offers on the network, the more that could go wrong or be possibly exploited. Additionally, the web service had a cross site scripting attack vulnerability, a minor issue but none the less a vulnerability. The cross site scripting attack is done by using the device as a way to send unsuspecting web browsers different information than the site being viewed. For more information, see: http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf or http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html.
- VENDOR 3: This vendor's telephone didn't have the SNMP problem, but did have a web server loaded. There did not appear to be the cross site scripting vulnerability on the service.
- VENDOR 4: This vendor's telephones also had the SNMP. This vendor's telephones also had the SNMP issues that were present in the vendors mentioned previously.

System Features and functionality

The following system functions and features were evaluated and discussed with vendors. All vendor systems were capable of performing these functions unless noted.

ANALOG PHONE FEATURE FUNCTIONALITY

- Extension to extension transfer
- Extension to trunk transfer
- Trunk to trunk transfer
- Trunk to extension transfer
- Conference calling/3 way
    - One vendor's system was unable to place conference calls of any type without enabling "multicast" on the data network.
    - On another vendor's systems it was somewhat difficult at first to make conference calls using the screen prompts, but once a couple calls were made, and the screen layout was understood, conference calls became much easier.
- Voice mail
- Message waiting light on analog phone
- Caller ID on Analog phone
- Remote voicemail retrieval
- Call Park/retrieval

HARDPHONE FEATURE FUNCTIONALITY

- Extension to extension transfer
- Extension to trunk transfer
- Trunk to trunk transfer
- Trunk to extension transfer
- Conference calling
- Voice mail
- Message waiting light on IP phone
- Message waiting light on analog phone
- Caller ID on IP phone
- Remote voicemail retrieval
- Call Park/retrieval

EASE OF HARDWARE INSTALLATION

- PSTN trunks
- Softphone extensions
- Hardphone extensions
- Analog extensions
    - While some systems were easier to configure than others, all could be configured relatively quickly by an experienced PBX administrator.

EASE OF CONFIGURATION

- Static or DHCP addressing
- PSTN analog trunks

- PSTN direct inward dial trunks
- Softphone extensions
- Hardphone extensions
- Analog extensions
- Voice mail boxes
- Auto Attendants
- Button configuration
- Automatic Route Selection patterns
- Local PSTN termination
- Remote PSTN termination
- Local IP termination
- Remote IP termination
- 911 routing
- Forwarding
    - RNA Ring no Answer
    - Busy
- Pickup groups
- Paging

REMOTE SOFTPHONE ACCESS

- Voice quality using Dial-up Internet
- Voice quality using DSL
- Voice quality using cable modem
    - Softphone voice quality was acceptable using DSL and cable modems however because of the limited bandwith using Dial-up internet connectivety voice quality was usually poor. It is important to note that even while using DSL and Cable modem, call quality is still at the mercy of the ISP's network and their congestion at the time.

SMDR

- Central system maintains common SMDR file for all remote systems
- Daily "push" SMDR to a remote server
- Accuracy of SMDR records
- Single record for IP calls between remotes
    - All systems tested had either onboard SMDR logs, or traditional SMDR ports for use with third party call accounting systems. Most of the smaller systems were not able to provide single call records for calls between remote sites.

DEVICE INVENTORY MANAGEMENT

- Report generation of all active devices, i.e. trunks, phones, VM ports

FEATURE INVENTORY MANAGEMENT

- Report generation of all assigned devices and features

FRAUD CONTROL

- Trunk to trunk transfer prevention
- Does system prevent Outbound calls from voicemail server
- Password login required for IP phone boot up
- Methodology to prevent unauthorized move of IP telephones

E-911

- Using PRI, ability to present actual station number to PSAP
- Capability of interfacing directly with ALI database
    - While some of the vendors tested provide additional software and hardware to support this function, none was provided for the test.
- Is your system capable of keeping track of phone sets that are moved from building to building and updating the ALI database without administrator intervention?
    - While some vendors provided ways of tracking telephone set movement, none was fool proof and the ultimate responsibility of keeping ALI database information up to date rests with the telephone system administrator
- Handling of E-911 on remote softphone access
    - Softphones were capable of placing 911 calls however most vendor systems were capable of blocking 911 calls from softphones. There is no automated way to ensure correct ALI information is sent to the PSAP when softphones are used from remote off-net locations.
- Notification of onsite personnel when 911 is dialed
    - Most systems tested were capable of notifying onsite personnel in the event of a 911 call

MEASURED UPTIME

- Device
- PBX system
- PSTN connections
- WAN connection
    - All PBX's, end devices, WAN, and PSTN connections remained relatively stable however, they were at the mercy of the network equipment. Any time a router, switch, CSU, or any other network device experienced trouble, voice quality or service altogether was compromised.

QOS

- Built in QoS or network provided
- Type of QoS optimal for system
- H.323 or SIP technology
    - While some of the systems or telephone sets were capable of providing their own QOS, QOS must be configured on each and every device on the network in order to operate successfully. If calls pass thru a half dozen routers, and even one is not configured for QOS, call quality will suffer during periods of high usage.

DISASTER PREPAREDNESS/RECOVERY

- Redundant processors
- Ability to install a second system on WAN to take over complete call control in the event primary system failure
- Operating system backup, i.e. tape drive, LAN/WAN storage, etc.
- Ability to completely erase and restored data within 30 minutes from backup
- Time it takes system to become fully operation after power loss and restoration

- Automatic recovery after power loss or intervention required
    - All systems came equipped with various backup strategies all of which were acceptable.
    - Of the systems tested only 2 had redundant onboard processors. Some systems relied on a second independent processor for backup.
    - All systems tested were capable of rebooting in the event of a power failure within an acceptable amount of time without Administrator intervention.

Test calling

All vendor telephone sets presented proper ANI to the PSAP when test calls were made with the exception of one. In that particular telephone, a programming parameter was evidently set to send a "test" number on caller ID delivery, and that test number was presented to the PSAP.

With directed traffic some of the systems had issues, leading one to believe that there was a possibility the traffic actually interfered with the VoIP traffic. The tests included additional traffic passed the same exact path/ports as the telephone traffic, but was not aimed at the telephone. The majority of the systems handled the calls just fine. The tests were brief and not as complete as they could have been with additional time. From a network perspective, it might be more difficult than first expected to protect IP phones from unwanted traffic. Isolated or limited access vLANs might be reasonable. However, unplug the telephone & plug your PC into the port or configure your PC to talk vLAN headers and it will probably be in the phone vLAN. Port/MAC address locking also be a feasible option, but difficult to manage when faced with a campus full of it. Limited access vLANs would typically be protected by a firewall or router access list (ACL), but without packet content filtering, which neither typically would do, a DOS on the same port number, would probably get through. Frankly, protecting VoIP phones and call managers from network traffic will require special planning and rigor.
The models we initially received were not hard to setup. While some of the telephone systems were initially shipped to us with the wrong IP configuration, it was intuitive enough to reconfigure them manually. Next came telephone usage. Many of the tests were concerned with the data side of testing the voice over IP telephones and how that affected quality. These were rated on a scale from 1 to 5, with 1 being the worst and 5 the best.

There were three tests done to evaluate data loads from the network. All were without QoS. First was same vendor VoIP system ---> VoIP system. A low data rate from internal traffic was acceptable. There were sporadic drops of voice in the first few seconds the load was applied, but it did recover to normal levels. When being hit with a high load of traffic, all voice was killed – nothing could be heard.

The next test was regular telephone--->VoIP system. When doing the moderate network load, the packets were dropped more often. Even after the load had continued, the

conversation was still understandable. But was annoying at times. The high load for this type of traffic also killed the conversation.

The final testing done with the vendor IP system was to the other vendor's IP telephone. The results for this test were the same as with the regular telephone to the VoIP telephone.

E-911

In order to understand the relationship between VOIP and E-911, we must first understand how E-911 is designed, how it works, and its limitations. Most 911 call centers in the State are E-911 capable. This means that when a caller dials 911, the dispatcher answering the call receives two pieces of information. The first item is Automatic Number Identifier (ANI), which is the callers telephone number. The 911 operator uses the ANI to call the party back in the event that the call is disconnected. ANI should be the actual telephone number of the person making the 911 call. The second piece of information is the ALI, or Automatic Location Identifier. ALI information contains the actual street address where the ANI is assigned. The ALI is kept in a separate database typically maintained by either a third party or the telephone company itself. When a call comes into the 911 Center, the ANI is received by the computer system controlling the calls at the same time the call is handed to an operator. When the computer system receives the ANI it connects to the ALI database and begins to query for the caller's physical address. The ANI and ALI information is then presented to the operator so that they can route the appropriate emergency personnel to their location as they are speaking to the caller. Simply put, inaccurate ANI and/or ALI information could at the very least slow the response of emergency service, or at worst, contribute to the loss of life.

The key to reliable E-911 lies in two areas. The first is to deliver accurate ANI to the 911 Call Center, and the second is to ensure that the ALI database is programmed with an accurate street address for every ANI. From the PBX perspective, accurate ANI delivery is most easily achieved by using properly configured PRI trunks. With PRI trunks the actual extension of the caller is converted into a 10 digit ANI by the PBX prior to sending the call out on one of its trunks. With any other type of trunking, it would be nearly impossible to send the actual ANI to the 911 Call Center. This is true of both traditional PBXs as well as VoIP systems. Accurate ALI information is achievable only if the database is set up properly during initial install, and updated each time a station is moved from one location to another. Here is where it can become complicated with VoIP. As discussed previously, many VoIP systems users have the ability to log into any telephone on the network using their own telephone number and their assigned password. This creates a situation where they can be logged in from a location that is different from that of their assigned telephone set. This location may be in the same building, another building, or even another State. The ANI information indicates the telephone number that is looked up in the ALI database giving a location that may or may not be the actual physical location of the caller. This could create erroneous information being distributed to emergency responders.

Additionally, with this new technology comes the "mobile worker" With many of the VoIP systems tested, users can install "soft phones" onto their workstations, laptops, or even their home personal computers (PC's). This creates an even bigger problem with 911 because emergency calls can be placed from just about anywhere in the country, yet they will terminate to the 911 call center closest to the physical location of the PBX. Again, the mobile worker could be in a completely separate building or facility from the PBX and the ANI and ALI information would indicate erroneous information on a e911 call.

Last but not least comes the "wireless VoIP telephones". While not all that different in this case from their traditional PBX relatives, they can pose additional problems for 911 callers. As in the case of a softphone or a mobile user, wireless telephone sets can be a problem even if the system is properly configured, and accurate ANI is delivered.

To resolve this issue, some systems can be configured so that the ANI being delivered to the 911 Call Center is tied to the actual switch port from which the call originated. In these cases each data switch is mapped to a particular floor and building address. Then, when emergency calls are placed, the system outpulses the ANI associated with the particular port where the call originated. When properly deployed, the ALI database will have been configured with street address information that matches the ANI sent from each particular data switch. To assist 911 Centers in obtaining the callers exact location, some systems can be configured to send a different ANI for each independent data switch port. While this could be somewhat effective in helping the 911 operator know the ANI's exact location, it would require that every data switch port be cross connected to a jack, that every jack location be assigned an ANI, and that each ANI be populated in the ALI database with its proper physical location. Although this sounds as if this could work well, but it would require that each possible jack location be cross connected to its own port on a data switch, and this is not typically done. The added expense of providing a dedicated switch port for each jack location may be cost prohibitive. If the system is using "Power Over Ethernet" then the end user would probably need to add a year to the return on investment figures.

While E-911 and VoIP has been a hot topic among 911 call centers, the telephone companies, and the various vendors, it is important to point out that many of the same problems exist with traditional non-IP PBX's and key systems if not administered properly. These problems are potentially compounded by the use of VoIP, but not insurmountable.

IP Centrex

Many of the KPST participants rely on Centrex from the local exchange company, Frontier Communications, for their telephone service. The pilot project did not include the testing of IP Centrex. Some discussion, however, was held on the Centrex telephony service offered over a managed Internet Protocol (IP) network. IP Centrex's delivery of services will be monitored as trials and implementations at customer sites are completed.

Regulatory Considerations

When discussing VoIP and its associated regulatory ramifications, it is important to make a clear distinction between private network based VoIP, LEC provided IP Centrex, and some of the other flavors of local service deployed by various companies over the internet who have little or no regulatory oversight.

With network based VoIP, regulatory considerations at present are typically no more than those encountered with traditional PBX networks utilizing "tie trunks" to connect offices. In the past, PBX administrators routed traffic from city to city using standard TDN tie trunks in order to save on toll charges. This made it possible for companies to save money in cases where there were significant amounts of usage between offices. In many of these cases calls could be handed off to the PSTN at the remote end making it possible to further leverage the TDM network. This allowed companies to save money on not only PBX to PBX traffic, but on city to city traffic as well. By comparison to VoIP, this practice was somewhat rare due to the added hardware and monthly recurring costs involved. With VoIP, this practice has become much more economical, and is growing at a substantial rate. If this practice continues to grow at its expected rate, the effect on originating and terminating revenues for the local carriers would become remarkable.

Not only does this toll bypass solution affect the long distance carriers' bottom line, but it could have a recognizable impact on Universal Service Funds as well. As the market share of long distance traffic begins to shift from public carrier networks to privately owned VoIP networks, regulatory bodies have begun to look at imposing regulatory fees for this type of traffic. This is evidenced by recent regulatory cases in Minnesota, California and Wisconsin. Questions are being asked about whether the services is voice or data? Is it subject to the same E-911, USF, PICC, and federal access charges as traditional service? As new fees are imposed on toll bypass calls, the added cost should be considered as the development of return on investment figures are made for VoIP.

With LEC provided IP Centrex, an end user's PBX or Centrex service is replaced by a LEC maintained local VoIP network. With this type of service, the same possibilities can exist for toll bypass. The major difference is that routing of traffic is much more tightly controlled by the LEC rather than your PBX/private network administrators. Carriers will know where your calls originate and terminate, and could easily use that data as a vehicle for collecting additional fees like USF should regulatory bodies make such a mandate. As local certified carriers begin to deploy IP Centrex, they are faced with the same return on investment issues as those with private networks, and that is; "how much will it cost to deploy the service".

Finally, VoIP technology can be provided by Internet telephone service providers. After several attempts to contact five different providers of this service, only two companies participated in a dialogue with the KPST team. Most of these companies offer flat monthly pricing which includes a private telephone number, switch, and unlimited long distance calling. For clarity, the switch mentioned is a device that would be mailed out that would provide connectivity between the Internet and a standard analog telephone set. The service requires a high speed Internet connection. However, the technical knowledge

of the sale representatives for this service was less than desirable and much of the information provided had to be interpreted and "reasoned" through in order to understand how the service worked and the quality that would be provided. As described, the KPST participants reasoned that an analog trunk port could be connected to the switch and used for toll bypass, or an overflow trunk in the event that the PSTN lines were full or out of service. Again, this group of providers do not bill regulatory fees. They are not certificated, regulated telecommunications carriers. The "voice" service is technically "data" service and therefore not subject to any of the same regulatory fees as other telephone service providers. The quality of service varies but follows the old adage of "you get what you pay for".

The following items are of particular concern, and will followed closely as VoIP continues to develop and be deployed.

E911 -

1. The lack of any industry guidelines and/or rules and regulations prevent standardization as to what telephone number will be associated with a VoIP call sent to a PSAP.
2. Without this standardization, the level and accuracy of information available to a PSAP for a VoIP call is unknown and therefore the level of response can not be quantified.
3. Guidelines or rules and regulations should be established to standardize what telephone number will be provided to the PSAP and how that number will be related to the ALI database.

Regulation of VoIP may be necessary to:

1. Provide the end user a minimum level of Quality of Service and means of resolving billing issues.
2. Provide the local exchange carrier means for reasonable access and termination compensation.
3. Ensure a level playing field and competitively neutral application of USF and E911 fees.

More Questions Raised

One item questioned was connectivity that performed the same function as the PSTN, but without the PSTN. Could the vendors have defined tie-lines or trunks between the call managers over the network, i.e., IP based? Calls could have been switched between call managers without the PSTN, if technically feasible. This may be important as different entities deploy VoIP with different vendors. It may make sense to "bolt" call managers together over the network as opposed to the PSTN.

It would be beneficial to have a better understanding why some of the telephones responded the way they did to directed traffic. The assumptions are that a) the vendor's handsets were simply not hardened enough to deal with the directed traffic, or b) the traffic actually interfered with the VoIP traffic. Dismissing b for the moment, what if the handset is a simple configuration of "partitioned" hardware, a network interface module

that examines all network traffic. If the network module is highly optimized and built around customized an Application Specific Integrated Circuit (ASIC), it would be able to look at a packet, determine it was not VoIP, and throw it away or determine it was VoIP and pass it on to the phone. Compare that with a model built around many older mini and microcomputers (70's – early 80's). There is one CPU, executing software, not firmware or microcode. This CPU does all processing including moving data in and out of input/output (network) interfaces. Load it up and it simply can't keep up.

Lessons Learned

The bullets below represent the information and comments made by the KPST participants related to VoIP technology and the application of this technology as an overall solution. As VoIP is moved into the network of an organization, some of these comments should be adopted as a "best practice".

- VoIP is not just another computer "network" component. This pilot brought to light the fact that massive attention and effort needs to be paid to the public switched telephone network. Configuring the PBX's for IP phones and users is a much smaller part of the deployment. Anyone with a VoIP system needs to have contracted maintenance or have someone who knows about copper, analog PBX's. Deploying VoIP means that you have to do all the PSTN "stuff" that you did with the older era PBX's.
- Early on there were comments such as: "remember I'm just a data person or remember I'm just a voice person". In implementing this technology we learned that it really takes both sides. You need sufficiently trained personnel in both areas to get it configured correctly and keep it continually working smoothly with a high rate of quality.
- Most of the data networks in operation are "best effort" networks. They can tolerate "some" degree of downtime. Voice networks operate differently. These networks introduce new subjects into the networking environment that deal with quality of service, network design and troubleshooting. Many of these functions today are performed by the telephone company. Entities that deploy VoIP must take great effort to assure that the network people can deal with network support of VoIP. VoIP or analog, it is still phone user support and configuration. Today, the network staff probably has absolutely no need to be involved in VoIP other than when it comes to designing and supporting the network for call quality. Under VoIP that could/would change or an additional staff would need to be hired to handle the voice "stuff".
- At the risk of ruffling feathers, I would speculate that the majority of network support personnel have had only minor experience with "in-depth" troubleshooting. It appears that 95%+ of all poor network performance issues are from "the grossly obvious." Granted many times locating the pertinent "grossly obvious" item may take some time. But during the identification of an obvious problem, the issue is that something is misbehaving (failing), overloaded or misconfigured. In the VoIP pilot, a number of vendors pointed out they have jitter tests, etc. The tools locate the jitter as a problem between two switches. But suppose neither switch has an "obvious" misconfiguration, a device producing

detrimental traffic or other symptoms typically found in virtually all situations. How many network support personnel actually have the experience of using the output of a "show process CPU" or "show process memory", etc. type of command to resolve a problem?

- There is a lack of any industry guidelines and/or rules and regulations that provide standardization as to what telephone number will be associated with a VoIP call sent to a Public Safety Answering Point. Without this standardization, the level of accuracy of information available to a PSAP for VoIP is unknown and therefore the level of response can not be quantified. Guidelines or rules and regulations should be established to standardize what telephone number will be provided to the PASAP and how that number will relate to the ALI database.
- VoIP needs to be a policy decision, as much as a technical decision. An awareness of the possible economic impact to communities where widespread VoIP deployment occurs needs to happen. In the case of a large community, a few thousand lines moved from a carrier network to a private network isn't likely to cause an alarming difference to a carriers bottom line. However, in a community like Kearney, Nebraska it could. State government is a large "anchor tenant" to many of the smaller rural communities in Nebraska. By "cherry picking" this traffic from the provider of last resort, unintended consequences could occur for the rest of the community.
- Decisions made about configuring communications service could cause economic hardship for other municipalities in the area. For example, many of the public services we depend on, such as 911, are funded through surcharges on telecommunications services. In Kearney, if the entities participating in this pilot were to convert their current contracts to a privately operated VoIP service, Buffalo County would loose over $1,500.00 per month in surcharge funding. This could place additional financial burdens on local municipalities, residents, or businesses.
- Policy decisions related to the regulation of VoIP also need to be made. Issues need to be resolved regarding: end users needing a minimum level of Quality of Service; a means of resolving billing issues; local exchange carriers having a means for reasonable access and termination compensation; and ensuring a level playing field and competitively neutral application of USF and E911 fees.
- As a former ITS director, used to say, "If the computers are down they really CAN still use pencil and paper. As we all know - if the phones down, duck."

VoIP Pilot @ Kearney