IPCOMM2006

September 25-27 • Gaylord Opryland • Nashville, TN

Disaster Planning: Tackle the Unique Challenges of IP Systems

Dave Chapman

President

Chapman Consultants

IPCOMM2006
September 26-27 • Gaylord Opryland • Nashville, TN

What Will Be Covered

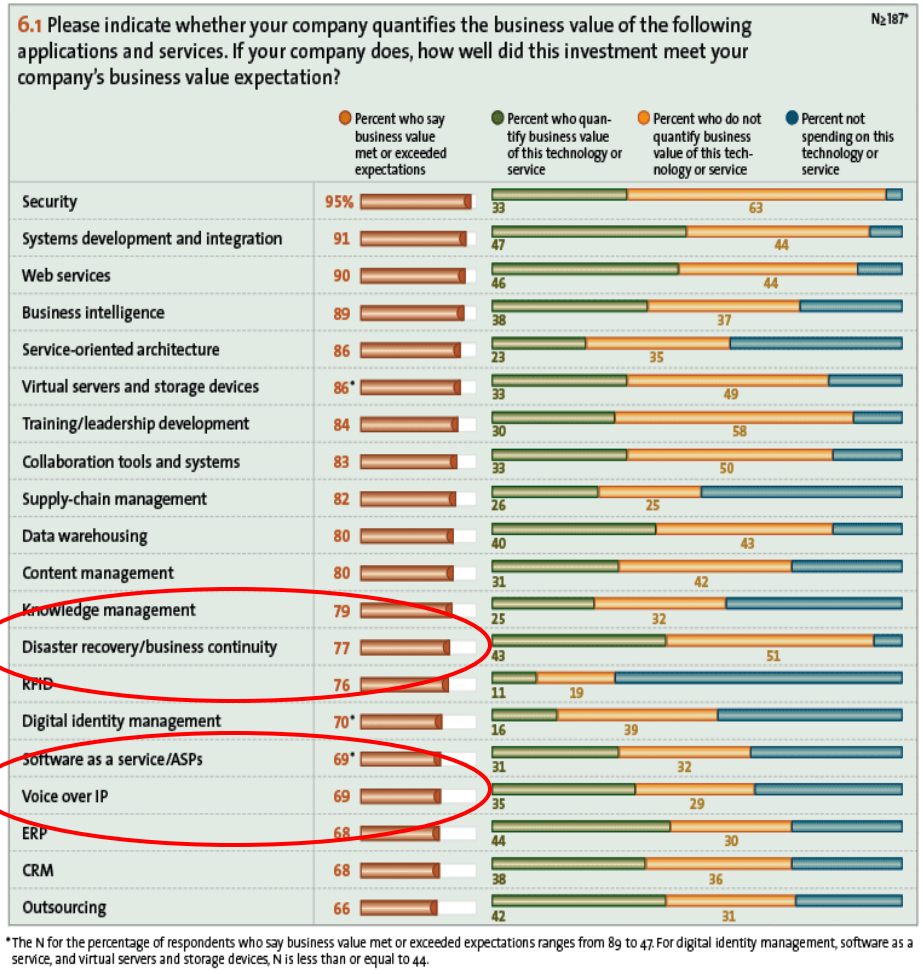
- Expectations put on VoIP
- What does a disaster mean?
  - Business impact
  - The cost of preparedness
- Design considerations for Disaster Recovery
- A real world example
  - Emergency Operations for Anne Arundel County MD

Expectations

- Voice services, whether traditional or VoIP are among the most critical of any IT services a corporation uses
- The ability to communicate with your co-workers and customers supports almost all other functions in the business
- When it's down, the IT organization is under tremendous pressure to correct it
- The longstanding impression that traditional voice is "always there" leaves a higher expectation on VoIP

IPCOMM2006
September 25-27 • Gaylord Opryland • Nashville, TN

Expectations – Business Value



6.1 Please indicate whether your company quantifies the business value of the following applications and services. If your company does, how well did this investment meet your company's business value expectation?

N≥187*

	Percent who say business value met or exceeded expectations	Percent who quantify business value of this technology or service	Percent who do not quantify business value of this technology or service	Percent not spending on this technology or service
Security	95%	33	63	
Systems development and integration	91	47	44	
Web services	90	46	44	
Business intelligence	89	38	37	
Service-oriented architecture	86	23	35	
Virtual servers and storage devices	86*	33	49	
Training/leadership development	84	30	58	
Collaboration tools and systems	83	33	50	
Supply-chain management	82	26	25	
Data warehousing	80	40	43	
Content management	80	31	42	
Knowledge management	79	25	32	
Disaster recovery/business continuity	77	43	51	
RFID	76	11	19	
Digital identity management	70*	16	39	
Software as a service/ASPs	69*	31	32	
Voice over IP	69	35	29	
ERP	68	44	30	
CRM	68	38	36	
Outsourcing	66	42	31	

*The N for the percentage of respondents who say business value met or exceeded expectations ranges from 89 to 47. For digital identity management, software as a service, and virtual servers and storage devices, N is less than or equal to 44.

- CIO Insight, August 2006
- 77% believe they get business value from Disaster Recovery/Business Continuity investments
- 69% see the value in VoIP!

Enterprise: Business Impact

- For most Enterprises a disaster means lost revenue
  - Temporary loss or degradation of productivity
  - Loss of product or service delivery capability
  - Disconnection from customers
  - Worker safety concerns
- Many enterprises can calculate lost $ per hour of downtime for system

Public Safety: Business Impact

- For public safety, downtime can mean lost lives
  - No matter where I am, when I call 911 they can help me
  - Police and fire can be dispatched 24x7
  - Police and fire can call for backup
  - Additional resources can be called in
  - Officials can get updated in real-time *during* disasters
  - Some would say disasters ARE Public Safety's business

Reliability - Enterprise

Reliability is a cost/benefit analysis for each “service” the company offers

- There may be an acceptable amount of downtime before business suffers
- Solutions can range from complete redundancy with live backup datacenters, to a prayer that nothing bad will happen
- May choose not to be “reliable enough” to manage a particular disaster
  - Some disasters may mean you don’t have any customers

Reliability – Public Safety

Cost/benefit is pretty straight forward

- Services that are life or death must be supported
  - Others are often ignored during a time of disaster
- Police/fire are expected to pull out all the stops to keep things operational
- Redundancy for key systems is paramount

Cost - Enterprises

Disaster preparedness viewed like insurance

- Most enterprises can afford a specific level of protection for each “service” but cannot afford to support “ultimate” redundancy
- There are businesses who don’t see the value in paying for “insurance”
- Semi-regulated businesses are required to have a specific level of operational capability, regardless of the disaster

IPCOMM2006
September 25-27 • Gaylord Opryland • Nashville, TN

Cost – Public Safety

"Customers" of the agency (ie: taxpayers) *assume* that services will be available in disaster situations

- Budget however is typically limited by those same taxpayers
- There is limited or no visibility into reliability or the cost of reliability from the taxpayer perspective
- Federal dollars are now much more available to fund local disaster preparedness following 9/11
- Some agencies pursue reliability of services at all costs, to the detriment of delivering other services

Cost in General

- In some cases the proper reliability may make a system cost 2-3x what a “normal” system might cost
- I like to say:
  - “The last 1.999% of the “99.999% uptime” will cost you more than 2x what the first 98% did!”
- This is why a cost/benefit analysis is so critical for the bottom line of any business
  - Ask yourself questions like these:
    - If 50% of your phones don’t need to be up 99.999% do I need a system to support them?
    - If a hurricane is big enough to take down my datacenter for 3 days, will I actually have customers during those 3 days that will call me?

Design Considerations

- System design should reflect the types of disaster you hope to be prepared for
- Some questions to ask:
  - Do you absolutely need 99.999% uptime?
    - Do you need it everywhere?
  - How long can you be out unexpectedly?
  - Which portions of the business can afford to be out more than others? (if any)
  - What types of outages do I need to be prepared for?

IPCOMM2006
September 26-27 • Gaylord Opryland • Nashville, TN

Design Considerations: Physical Disasters

- When preparing for facilities that are destroyed or damaged you must plan for remote site operations
- There are 2 types of facility destruction you have to be prepared for:
  - Datacenter
  - End-user spaces
  - Both!

DataCenter Damage

- At a high level, with VoIP you have 3 choices:
  - A hot-standby remote datacenter
    - Load balancing operations a consideration
  - A cold-standby remote datacenter
  - A “leased service”
- When the datacenter is co-located with office space the backup datacenter must be capable of supporting backup office space
  - Note that with traditional voice, the PBX is almost always with the office space
  - Supporting backup office space with a traditional PBX may mean a new PBX and new phone numbers
- Small remote sites may be supported with backup systems that are not possible with traditional PBX
  - For example Cisco’s SRST (Survivable Remote Site Telephony)

DataCenter Details

- External phone connections
  - External numbers are unavailable when the site they connect to are down, even with VOIP
  - VoIP is extremely flexible, but PSTN gateways connect to “Fixed” phone lines
  - Consider multiple terminations for the PSTN connectivity
  - 800 numbers are easier to re-direct, but may take time if not planned ahead
- IP is an advantage *internally*, as it’s easy to re-route calls once on the IP network
  - With IP, an extension can actually be anywhere on the network *without* IT involvement
  - Changing the internal dial plan can be done yourself with no help from the phone company

Datacenter Details

- With larger environmental disasters, your datacenter might easily be repaired, but support services might not be available (PSTN, power, networks)
  - Might cause you to go to backup systems even if everything in the building is functional
  - You might not be granted access to the building in cases of a state of emergency being declared
    - Ask the folks affected by hurricane Katrina, even public safety organizations had a hard time getting contractors in to fix equipment
  - Obtaining fuel for backup generators will become an issue for longer-term disasters
  - BIG consideration for datacenters that support employees OUTSIDE of the disaster area

Datacenter Details

- Datacenter's dependence on power and telecommunications require redundant power sources and diverse telecom routing
  - Power requirements may mean two diverse routes as well as backup generators (don't forget the fuel supply!)
  - Double and triple check telecom routing, you may THINK you are getting diversity that is not really diverse
  - Same applies to VoIP systems that are not in a true datacenter, but a "computer room"
- Don't forget the cooling system
  - It should have extra capacity for individual units to go off line for failure or maintenance

Datacenter Redundancy

- Having a second datacenter in a distant location is just the first step!
  - PSTN connectivity planning is CRITICAL
  - Failover planning and testing is a MUST
  - The location must be far enough away that one event does not impact both locations (this is possible with VoIP)
- The most faithful design is a “load balanced” environment, where both datacenters are functional at the same time, and each can handle the full load when one fails
  - Requires no manual intervention, happens automatically
  - Obviously most expensive, and hardest to implement/operate
  - Not really feasible with traditional PBX

Datacenter Redundancy

- The next best thing is a standby datacenter
  - Requires some manual intervention, which extends or interjects down time
  - Requires regular and consistently updated synchronization routines
    - May be automated
  - Less costly, but takes longer to get up and running
  - The telecom infrastructure must be in place and operational
  - This is a service offered by many 3rd party vendors
  - Again, a possibility because of VoIP

End-user Space

- When the end-user space(s) are confronted with a physical disaster different factors are at work
  - Most enterprises cannot and do not have redundant office space for an entire staff
  - Workers themselves must be relocated, not just “bits and bytes” like a datacenter
  - If the datacenter is still operational, then it can all be done with IP!
    - The challenge is getting the new office space connected, after that, it’s practically automatic

End-user Space

- IP connectivity to the backup location becomes the critical factor
  - Is it a fresh, newly acquired site?
  - Is it a leased, pre-arranged site?
  - How long will it take to get a WAN link up?
  - Can you do it over the Internet with a VPN?
    - Yes, at least temporarily
- Phones and LAN gear the next factor
  - Are people locked to a specific phone, or are you doing “hotel” services, and any phone from the right vendor will do?
    - Possible with VoIP, but has to be planned ahead of time
  - Is phone configuration locked to MAC address?
    - Almost like the traditional PBX technology, if you are doing this, you are not taking advantage of VoIP!
- And of course you need the IT staff to put it all together

IPCOMM2006
September 26-27 • Gaylord Opryland • Nashville, TN

IT Staff and Disasters

- VoIP expertise is hard to come by!
- Don't underestimate the importance of managing an IT staff during a large-scale disaster
  - Remember, it's likely that they are personally affected by the disaster too
    - Families must be cared for
    - Personal property must be looked after
    - They get emotionally and physically worn down
  - Plan to give them assistance!
    - They may need a place to stay, food, help with family matters, transportation to and from work, time to re-generate, etc
  - Extra services and flexibility required at the office
  - Many might not be able or *willing* to come in at all

Backups

- Even with two datacenters, it makes sense to have off-site and on-site backups
  - Don’t forget that VoIP systems are spread of MANY components, unlike traditional PBX systems
- TEST your backups
  - Make sure they are valid
  - Make sure the staff knows HOW to do it
- Keep duplicates onsite for quick recovery, and off site for when the on-site is destroyed
- Secure them, they contain your business knowledge!

IPCOMM2006
September 25-27 • Gaylord Opryland • Nashville, TN

Quick Points for Large Disasters

- Determine business requirements ahead of time
  - Be realistic
  - Involve all aspects of the business, particularly facilities
  - Make sure everyone understands the COST
- Build a plan based on true business needs and budget
- Get “buy in” on the plan and the budget
- Build it!
- Test it, repeatedly and regularly
- Repeat all steps on a regular basis

Tricks of the Trade

- Maintain a small number of POTS lines for emergency use
  - Spread them throughout the facilities
  - Don't depend on them to be there ALL the time
  - Don't connect them to the VoIP system, make them direct phone company POTS lines
- Obtain a two way radio system for the IT staff to use during recovery
  - Helpful even in small disasters and for every day use
  - Will work even when cell phones don't

IPCOMM2006
September 25-27 • Gaylord Opryland • Nashville, TN

Self-Inflicted Disasters

- The good news is that they are typically "recoverable" if you have your act together

- The bad news is that most people will believe that you don't have your act together (even if you do!)

Preventing Self-Infliction

- Change control process
  - The number one way to avoid taking down VoIP on accident
  - The number of components in a VoIP system compared to a traditional PBX makes this crucial
  - Must have ALL aspects of IT involved
  - Must really analyze how each change will impact the VoIP system
  - Must be followed, don't be tempted to do something "extra" while you have your hands dirty
- Testing
  - Build as realistic a test lab as possible
  - Try each change you intend to make ahead of time

Preventing Self Infliction

- Proactive Monitoring and Management (network and servers)
  - Again, the complexity and “entropy” of a VoIP system makes this more critical than a traditional PBX
  - Capacity planning
    - Traditional PBX systems have a “fixed” performance curve VoIP does not
  - Fault monitoring
  - SLA monitoring
  - Simulations (Load testing)
  - Post-change “status checks”
    - Simulate calls
    - Automate configuration checks
  - Regular security scans

Recovery From Self Infliction

- Maintain “known good” configurations
  - Regular backups
- Know how to restore from backup
- Hardware maintenance
  - Spares
  - Good response time for equipment repair
- Communications with end-users
  - Proactive notifications
  - Follow-up updates

Vendor Induced

- Most of the time this is a circuit outage or power failure
  - Backhoe Fade!
- Might also be considered systems that are infected with a virus or just a major bug
  - Much more likely with VoIP systems
- Hardware failures
- At least you can shift the blame a *little* bit
  - But! Did you do your homework when you picked that vendor?

IPCOMM2006
September 26-27 • Gaylord Opryland • Nashville, TN

Preventing Vendor Induced

- Where possible use multiple vendors
  - Two connections to a site from different service providers
  - Careful about last mile, often they are supplied by the SAME local phone company!
    - Make sure it's TRULY a diverse set of circuits
  - Might also consider different types of physical connections (fiber and microwave?)
- Backup generators, and UPS from the datacenter to the edge devices
  - Use POE in switches for phone power to eliminate having a UPS under every desk!

Preventing Vendor Induced

- Maintain good service contracts
  - This can't prevent a hardware outage, but can limit your exposure by getting fast service
- Consider some "self sparing" when you have a lot of a particular piece of hardware in production, or when something is prone to failure
- Implement redundancy where possible and affordable
  - For example on some stock trading floors there are 2 PCs on every desk, each one connected to 2 separate switches in 2 different wiring closest connected to redundant routers… you get the picture!

Design Considerations –Public Safety

- For natural disasters, phones, systems and networks will be in highest demand when storm conditions are approaching their worst, and then in the timeframe immediately after a disaster
- Bandwidth requirements could more than double as police/fire resources are ALL called in for work
  - Assistance from outside communities increases need even further
- Large scale disasters easily destroy large portions of networks and data centers
  - Often requires the use of "non-traditional" layer 2 communications such as microwave to provide diverse routing
  - POWER requirements will mean generators and a means of delivering additional fuel

Design Considerations for Public Safety

- Redundant datacenters *may* be located a safe distance outside of the jurisdiction, but office space and communications **must** be locally maintained
- While SOME natural disasters have advanced warning, man-made disasters are far more unpredictable
  - Additional capacity needs to be available immediately, without ramp-up time
- IT support staff and vendor maintenance may be unavailable for periods of time
  - Often demands the ability to self-spare some parts

IPCOMM2006
September 26-27 • Gaylord Opryland • Nashville, TN

Anne Arundel County EOC

- AA County has a Emergency Operations Center that operates 24/7
- AA County is in central Maryland and home to several “critical” pieces of infrastructure
  - BWI Airport
  - Maryland State Capital
  - Chesapeake Bay Bridge
  - US Naval academy
- It’s also about 30 minutes outside of Washington DC
- Core components include an IP network, and VoIP telephony

AA County Backup EOC

- Early in 2005, the Director of emergency services had a vision of providing “redundant” EOC capabilities through the use of a “Mobile Command Vehicle”
- The vehicle had the following primary objectives:
  - Remain operational in the event the primary EOC is unavailable
  - Manage emergency operations using the National Incident Management System (NIMS) from a mobile environment
  - Stream video surveillance footage and have video teleconferencing capabilities from the Mobile Command Vehicle back to the Anne Arundel County EOC
  - Establish Interoperable Communications with any agency in the State of Maryland and jurisdictions the border Maryland
- Primary issue: “interoperability” among disparate radio systems during emergency situations

Communications Interoperability

- AA County chose the ARINC Wireless Interoperable Network Solutions (AWINS™) as the communications platform both within the vehicle AND in the EOC
  - Uses VoIP as a means of providing “radio interoperability”
  - Provides “anywhere” connectivity through the use of Satellite communications
  - VoIP provides the mobile communications, “portable” phone numbers, and ability to dynamically adapt to emergency situations
  - VoIP phones can now also communicate with radios

MCCU-1

AA County's Mobile Command and Control Unit 1 was introduced in the fall of 2005 with the following capabilities:

- Communications vehicle designed to allow for mobile communications and RF interoperability.
- Will allow for mobile communications and interoperability between 17 RF Systems (479 Frequencies-250 programmed), 20 IP Phones, and 10 POTS/Cell connections at one time.
- Other capabilities include Video Teleconferencing, Video Surveillance, and Data Applications

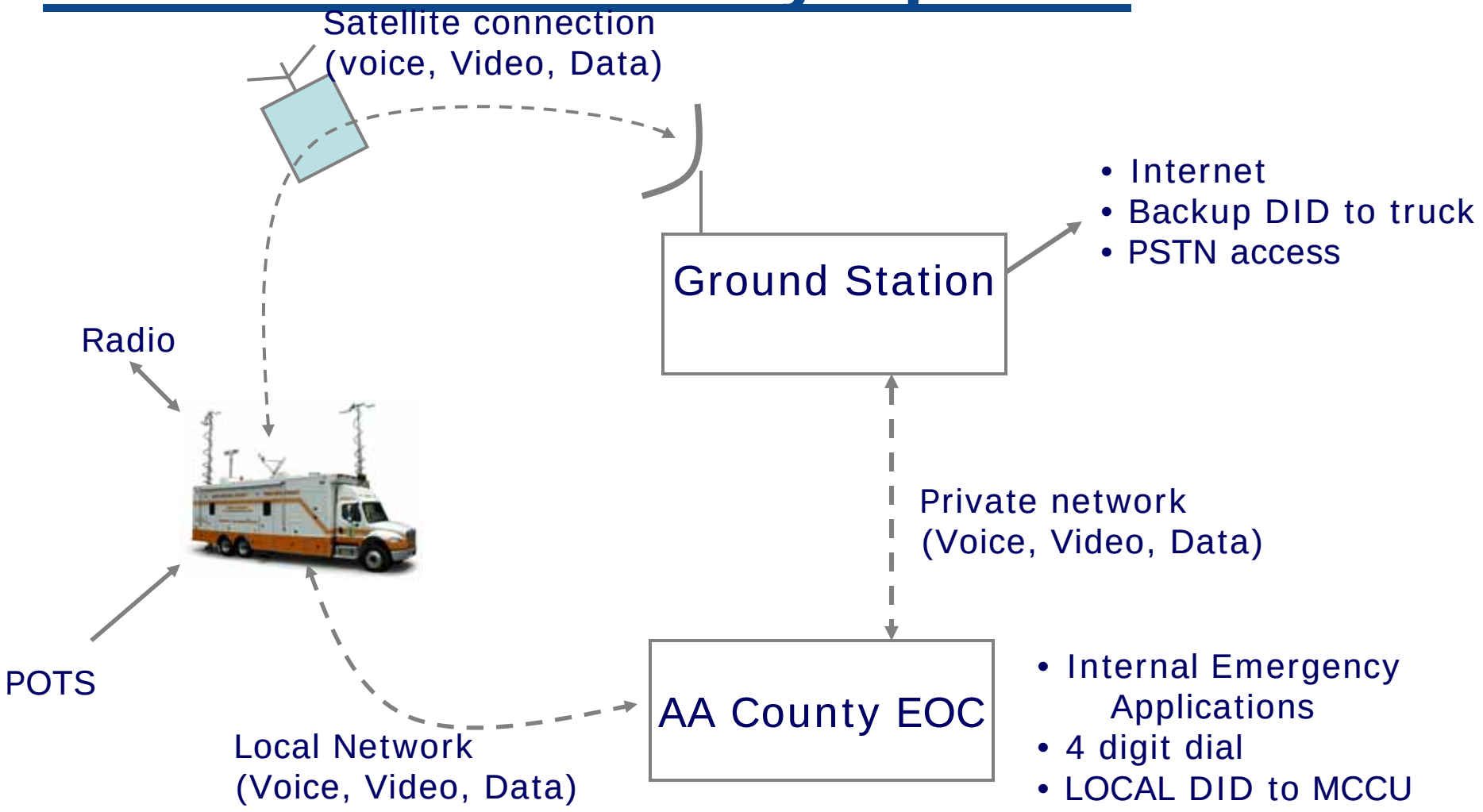
MCCU-1


ANNE ARUNDEL COUNTY
FIRE DEPARTMENT
MOBILE COMMAND
& COMMUNICATIONS UNIT
EMERGENCY MANAGEMENT BUREAU
MCCU-1

EOC Redundancy

- MCCU-1 is a backup EOC, in that all calls to the EOC can be re-routed to MCCU-1 in the case of an evacuation of the EOC
- It is kept in a physically separate part of the county from the EOC
- Completely mobile and capable of operating FAR away from any danger in AA County
- Connections via land line when available for telephony, and IP connectivity, or Satellite when required

Network Connectivity Options



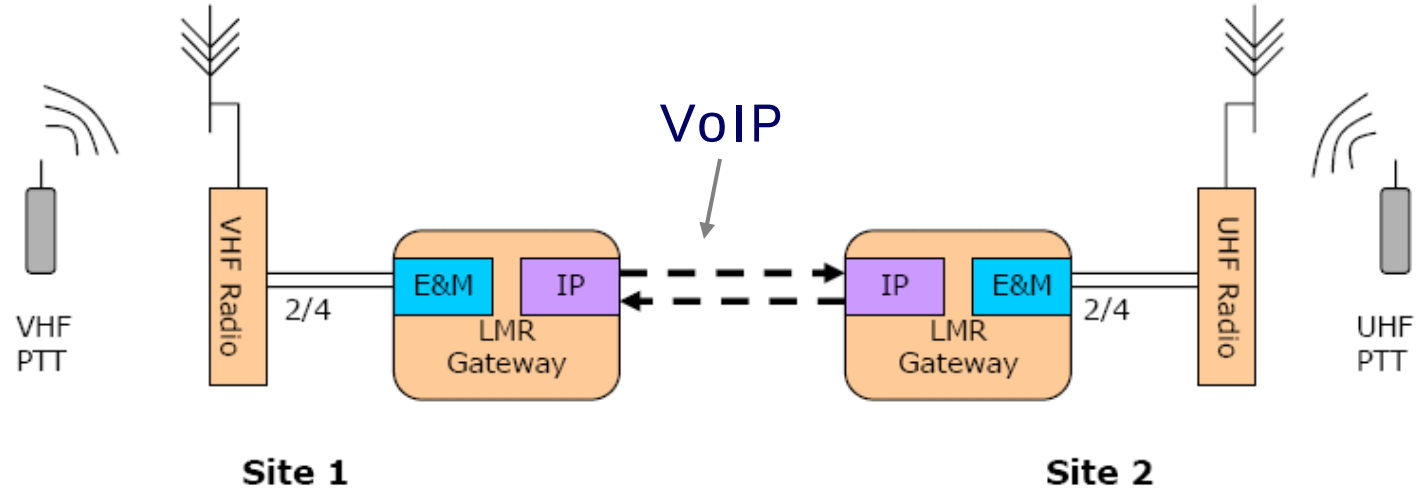
Redundancy IN MCCU-1

- Two racks, one on each side of the truck contain:
  - Fully redundant routers
  - Redundant switches
  - Redundant Land Mobile Radio gateways
  - Duplicate Cisco CallManagers
  - UPS
- Most popular Radio frequencies have 2 radios (supports up to 24 total radios in the vehicle)
- Ruggedized laptops
- 12 dispatch stations, where each user can use both a phone and laptop to communicate via RADIO AND VoIP

Dispatch Stations

Radio Interoperability

- Disparate Radios can communicate with each other via VoIP



- Also allows communications among:
  - Radios, cell phones, Nextel PTT, pots phones, VoIP phones, Video Conferencing

IPCOMM2006
September 26-27 • Gaylord Opryland • Nashville, TN

Hurricane Katrina Support

- MCCU-1 was deployed to Jefferson Parrish within 3 weeks of delivery to the county and was operational within 45 minutes of arrival
- Mission was to provide communications support for walk-in medical clinics
- Team consisted of 14 Maryland jurisdictions and 7 other groups (lots of different radios!)
- Easily met both the local communications requirements AND Video conferences, and telephone updates to Maryland
- Provided Internet access to all volunteers on the mission
- Operated flawlessly for more than 3 weeks, all on generator power

Operation Lifeline

IPCOMM2006
September 25-27 • Gaylord Opryland • Nashville, TN

Key Points to Take Home

- 3 basic types of disasters
- Planning a key requirement for success
- Develop a plan in concert with business requirements
- VoIP gives you flexibility INSIDE the network
- Still vulnerable to the reliability of the PSTN
- Even small increases in redundancy escalates cost significantly

IPCOMM2006
September 25-27 • Gaylord Opryland • Nashville, TN

QUESTIONS?

Contact:
Dave Chapman
Dave@chapmanconsultants.com
410 340 7597

CHAPMAN CONSULTANTS