

Incident Based Automation, IBA, System  
Business Process Modeling, Interview  
Incident Computer Technical Specialist, CTSP  
Type I  
December 06, 2006

Interview Notes by Craig Tanner, Data Modeling Architect

Historical changes and increase of capabilities (over last 9 years)

1. Previously, Type I teams did not have the position of computer specialist at all.
2. Complexity of computers and deployment has grown exponentially over the past 5 years. For example, from taking 5 computers to an incident to 30.
3. Many people who bring computer equipment to the incidents, sometimes as many as 30 additional computers that have to be networked, complemented by the number of printers, plotters, and all of the server and network equipment. "All of these computers are basically useless unless they are networked together."
4. Computer kit consists of 10 trunks of equipment which is hauled to the site, primarily in an SUV.

Question: What is the typical hardware and software configuration activity?

Answer:

1. Initial setup of network components based on historical and anticipated need
2. I-Suite tool has to be networked over many of these computers.
3. Although the configuration will vary with each incident, the basic configuration is for networked clients configured over a hard-wired network. These wires are run along the ground.
4. Replicate HQ configuration initially; each configuration unique, typically two servers
  - a. One dedicated I-Suite server - The I-Suite server contains historical data that is specifically for his particular team and contains their specific documents.
  - b. one SNAP server
    - i. configured with 40GB and repository for current and past incidents
    - ii. historical and current documents external to what I-Suite manages
    - iii. Use by mapping
      1. Radio Metric Tracking, e.g., helicopter is separate source of GIS data
      2. GPS units

Question: What is the role of the CTSP after setup?

Answer: Keep the network working, reconfigure based on changing requirements, take the network completely down for demobilization, and remove team hardware

components during a team rotation when CTSP is transitioning and ensuring capabilities for replacing hardware by the incoming CTSP.

Team Rotation - There are two types of team rotations for Type I teams:

1. Within an operational region, there are three Type I teams. These are rotated every week. Each team is on call every third week.
2. Nationally, there are 17 teams. Theoretically rotated every 17<sup>th</sup> week but not in play until activity (an incident).

The ordering of teams to an incident is determined by the complexity of the incident. The more complex the incident, the higher the level of the team. In other words, a local (Type III or less) team will usually be the first at an incident and if certain capabilities and resources are needed that are beyond theirs, the next higher level team is called in. A Type I team may eventually be called in from that region and others from the national rotation and other regions.

Question: How is the CTSP notified about an incident?

Answer:

1. Teams are typically alerted by phone and told where to go by the Dispatch Center, a “Resource Order”.
2. Drive to site with SUV providing a “standard kit”

Question: How does the CTSP manage the standard kit?

Answer: The kit of computers and equipment is prepared in the beginning of the year before the fire season; February through May, then September through December. The combination of computers, equipment, and human resources that are set up and operate this equipment is called a “Standard Kit” and is part of a “Resource Order” that is called for deployment.

Question: What are the processes of the CTSP upon arriving at site?

Answer: Generally, the computer support team arrives at or after the in-briefing and do not normally participate with the in-briefing. The primary concern of the CTSP initially is where to locate and set up and the coordination with the logistics section of the incident management team on putting the “small city” together based on whether local jurisdiction has a location, and a facility with adequate protection? The computer operations team must be in pretty close proximity (network can extend a maximum of 300 meters).

Question: What are the setup processes?

Answer:

1. The CTSP coordinates with Logistics to create network topography, with switches, for where units are located (Plans, Time, Situation leader, etc.)

- a. Available external connectivity may include cable, DSL, satellite, phone (fax); personal preference is for cable. Download and upload of GIS data is cause of load; 512KB band is acceptable.
  - b. Network configuration varies by serial daisy chain to star clustering
2. CTSP and a deputy are the two primary resources that perform setup. They must unpack all equipment and setup the entire network.
3. The “small city” at an incident is typically up and running within 48 hours. Depending on the location, the setup may be more difficult, e.g., trailer or tent.
4. Sometimes the site is already provided internet connectivity making the setup easier, normally providing better for the protection of the equipment.
5. Setup is typically a more complex task when taking-over the network from another team (described in more detail below).

Question: What are the steady state processes after setup?

Answer:

1. Steady state includes constant monitoring of the network, network changes (such as changes in physical configuration, and in the number and types of computers that are connected), and adding and maintenance of peripheral equipment such as printers and plotters. Sometimes the CTSP must reconfigure networks because computers are moved based on logistics needs (i.e. a trailer has to be moved). (An ad-hoc process, unique for each site.)
2. Monitoring
  - a. Involves using a browser to access router diagnostics and based on router features provided to track components on the network.
  - b. Software utilities provided by CTSP based on personal preferences
3. Network changes
  - a. CTSP receives requests from Logistics section, but also from other section chiefs
  - b. Sometimes necessary to make a network map after many (minor) changes requiring CTSP to walk the lines (Ethernet cabling configuration).
4. Troubleshooting
  - a. Troubleshooting typically consists of problems associated with network connectivity, I-Suite, and printers.
  - b. Finance gets priority

Question: What are the processes for team transitioning?

Answer: The maximum amount of time that a single team can remain on an incident is 2 weeks. This will usually necessitate a transition of teams. Also, an incident that changes classification (such as from a type 2 to a Type I incident) will require a transition from one team to another. The procedure is for the team transitioning out to pack up their own equipment and make way for the new team to deploy their own equipment. Since each team has its own equipment, they generally cannot leave it on location (this has happened in rare cases). The exception to this is when equipment has been rented and does not

belong to a specific team. The team leaving will generally leave the network wire in place for the team transitioning in.

1. Incoming
  - a. Replace equipment
    - i. Take inventory
    - ii. Rented equipment remains at site as does network cabling (CTSP must order new replacement cable for kit after returning home.)
    - iii. Snap server – copy relevant data to CD
    - iv. I-Suite replication - The data from the I-Suite server must be transferred to the incoming server. This is called “Stop and Copy” and means that people have to stop entering data for a period of time while the transition is made.
      1. Broadcast scheduled deadline for when I-Suite server will be stopped. Deadline is coordinated and, for example, is a deadline for Time Unit Leader.
      2. Stop server
      3. copy image
      4. replace hardware and restore with new image
      5. Start server
2. Outgoing
  - a. Upload I-Suite snapshot to Kansas City central repository when external network access is available.
    - i. Cable modem, DSL (dialup has been used under extreme conditions)
    - ii. Satellite network provided by Lyman Brother Communications (Salt Lake)
      1. Internet phones
      2. Share bandwidth between camps

Question: What are the processes for Demobilizing?

Answer:

The tasks involved with demobilizing typically begin when there is 100% containment or percent containment such that control is turned back over to local units (local jurisdiction). The entire camp must be taken down and packed up.

1. Packing and cleaning activities
2. Final upload to the I-Suite database to the central data repository
  - a. Copy of data to local team when incident is not done (? patrol status) some fire operations may still be ongoing and the I-Suite database may still need to be transferred to another team or a local team. Even if the local team will not be using I-Suite, a disk is given to them so that they have all of the incident data.
3. After Demobilization
  - a. When the CTSP returns home and, depending on how busy the fire season is, they take time to refurbish, clean and repair the equipment.

- b. “Resource Order” form for requisitioning replacement equipment (for things like disks, network wire, etc.).
- c. Steady state at home office
  - i. update software, mainly with patches for I-Suite
  - ii. create new images
  - iii. CTSP continually replaces equipment.
  - iv. Goal is to make the kit ready for the next incident.

Recommendations and Issues:

- 1) Bandwidth is an issue at many incidents. They have a large amount of GIS data that is being uploaded and downloaded in addition to all of the other traffic (external network bandwidth is 512 KB).
- 2) Develop a standard IT kit that would be delivered to the incident and ordered the same way other resources are ordered. This would eliminate the computer team from having to haul 10 trunks around with them and possibly cut their load down to 2 trunks. When the first Type I team arrives at an incident, the kit would arrive too (possibly this is contracted out). When the team leaves the incident, they exit without having to pack or replace.
- 3) Wireless network