Case Study

NCRnet: How the National Capital Region Built a 21st Century Regional Public Safety Communications Network

Public Safety and Homeland Security Bureau

Federal Communications Commission

August 25, 2009 Broadband Workshop

This case study describes NCRnet, which had the objective of interconnecting 19 jurisdictions in the Washington Metropolitan Area in a private, multi-functional fiber optic network for public safety communications. This very sizable undertaking was recognized in 2007 as the "Community Broadband Network of the Year" by the National Association of Telecommunications Officers and Advisors (NATOA). The following is a description of the case study, and highlights the features that contributed to the project's success:

NCRnet Case Study: How the National Capital Region Is Building a 21st Century Regional Public Safety Communications Network

In the period following 9/11, the local jurisdictions in the National Capital Region (NCR) came together to address the severe interoperability issues that had become apparent in the public safety response following that tragedy. The jurisdictions developed a vision for a crucial new public safety communications network to connect community leaders and first responders across the Washington, D.C. metropolitan area.

The goal of the NCR Interoperability Program (NCRIP) was to enhance the region's public safety and emergency response communications and systems interoperability through the establishment of a new fiber optic digital network. Through NCRIP, the region applied for funding from the federal Department of Homeland Security (DHS). Funding was awarded and NCRnet—a collaborative work of 19 jurisdictions in three states in the Washington, D.C. metropolitan area—was born.

Designed and deployed with a range of innovative digital networking technologies and IT security measures, NCRnet represents one of the most sophisticated approaches to regional interoperability currently in place in the United States.

NCRnet's Goal Is Public Safety Interoperability

The goal of NCRnet was for local government agencies and organizations to be able to seamlessly share critical data and information during emergencies and during day-to-day operations. Through stakeholder discussions and analysis of existing infrastructure, the region worked to create a government-controlled fiber optic network. NCRnet enables the interconnection of public safety databases, communications, and functions in order to manage regional incidents and emergencies. As part of an effort to build and improve interoperability of Emergency Support Functions (ESFs) in the region, NCRnet was designed to connect the existing NCR jurisdictional networks (many of them Institutional Networks or "I-Nets") to form a secure and reliable cross-jurisdictional institutional network and minimize dependence on carrier and service provider networks.

The Network Was Planned for Security, Reliability, and High Bandwidth

In 2005, the NCRIP assessed requirements for the network, and piloted an initial interconnection between the District of Columbia and Montgomery County, MD. The needs assessment demonstrated conclusively that local first responders and emergency support personnel needed a secure, reliable, regional communications infrastructure; in particular, regional video streaming and videoconferencing, applications that can best be supported over fiber optics.

The assessment established a number of design principles in consultation with stakeholders and on the basis of the needs assessment results. Among these:

- The ability to support a diverse community of potential users (first responders, public health, local, state, federal government, education) without conflict between the users;
- A robust, scalable, survivable network infrastructure that connects with each participant's own fiber network;
- The need to operate independently of leased carrier infrastructure, the Internet, the public switched telephone network, and the I-Net electronics of individual jurisdictions;
- The ability to interface with different network devices models and brands used by jurisdictions, using industry best practices and federal communications and security standards; and
- A platform for real-time interoperable data exchange between different users regardless of native applications and formats.

These design principles ensured not only that the developing network fulfilled regional needs, but that this would be achieved in a cost-effective manner.

The Network Was Built Using Local I-Nets

Local government I-Nets and various agreements for access to fiber optic cable are enormously valuable resources in designing a cost-effective, inter-jurisdictional, fiber-optic network. While some of the governing agreements underlying the I-Nets restrict the use of fiber, acceptable use is defined in a manner consistent with public safety usage.

I-Nets are well suited to public safety communications. Their independence from commercial carrier lines assures a survivable network when commercial options are saturated. In addition, local government control allows flexible network design, and end-to-end risk and security management.

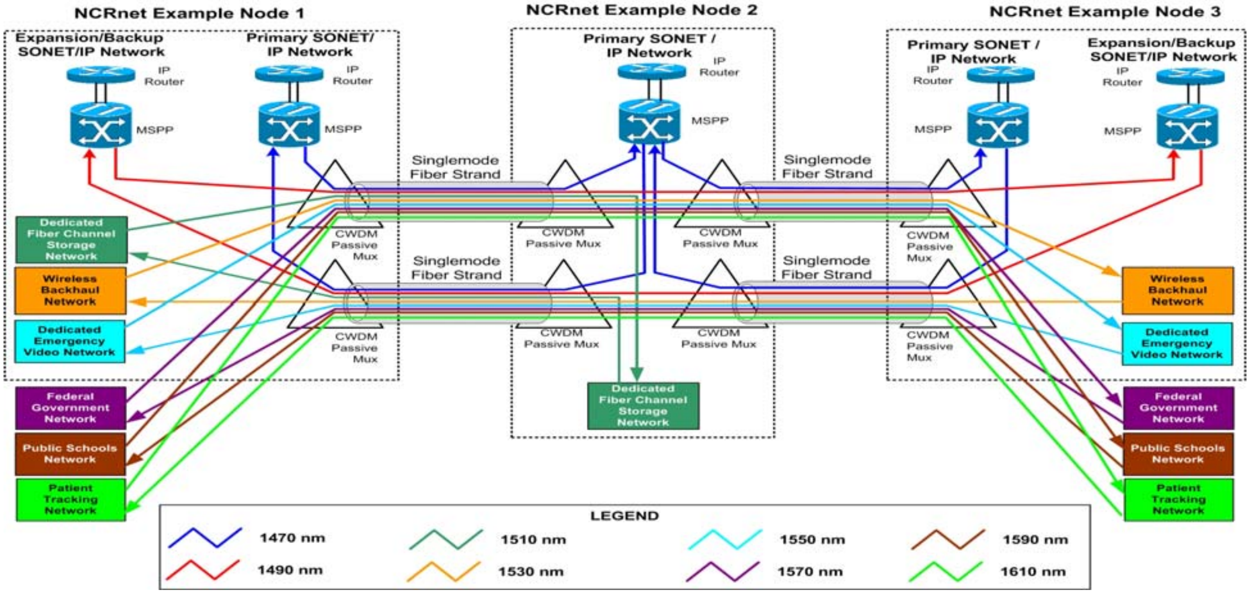
Previous work developing many of the jurisdictions' I-Nets formed the basis for NCRnet due to spare fibers in existing I-Net plants and provisions for rack space at potential hub sites, which allowed NCRnet to re-use existing assets. In addition, the NCR jurisdictions' agreements with cable providers typically had provisions for building out and extending I-Net footprints at advantageous cost (often to the mutual benefit of government and cable providers).

The Network Was Designed for Flexibility and Local Control

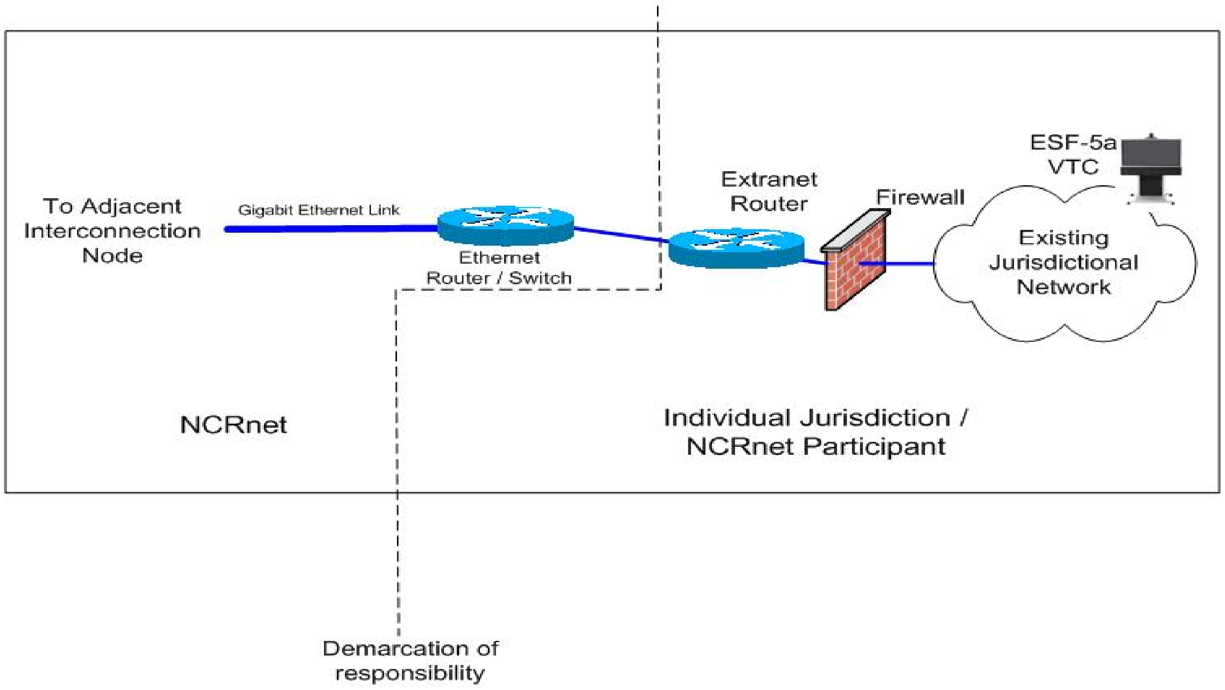
NCRnet's maximum flexibility reduced the need for future redesign or complicated network governance. The current implementation treats NCRnet as a "semi-trusted cloud"— a private intranet. Jurisdictions protect themselves with a firewall, and manage communications into their own networks with an extranet router. On the NCRnet side of the demarcation sits an Edge Router that handles traffic within the NCRnet cloud. NCRnet monitors only the equipment on its side of the “demarc,” while the jurisdictions are responsible for the equipment that controls access within their own networks.

The design allows both for relatively easy and incremental electronic upgrades – allowing additional capabilities for rapid fail-over, augmenting capacity, segmenting traffic, or applying sophisticated Quality of Service policies. This has allowed for a cost-effective implementation starting with a flexible IP-over-Ethernet 1 Gbps transport that can scale with funding availability and need. For example, an activated SONET ring around one of the key jurisdictions that allows rapid failover and increases continuity of operations was recently added.

Example Scalable Network Using WDM


NCRnet Example Node 1
NCRnet Example Node 2
NCRnet Example Node 3
Expansion/Backup SONET/IP Network
Primary SONET/ IP Network
Primary SONET / IP Network
Primary SONET / IP Network
Expansion/Backup SONET/IP Network
IP Router
MSPP
Singlemode Fiber Strand
CWDM Passive Mux
Dedicated Fiber Channel Storage Network
Wireless Backhaul Network
Dedicated Emergency Video Network
Federal Government Network
Public Schools Network
Patient Tracking Network
LEGEND
1470 nm
1490 nm
1510 nm
1530 nm
1550 nm
1570 nm
1590 nm
1610 nm

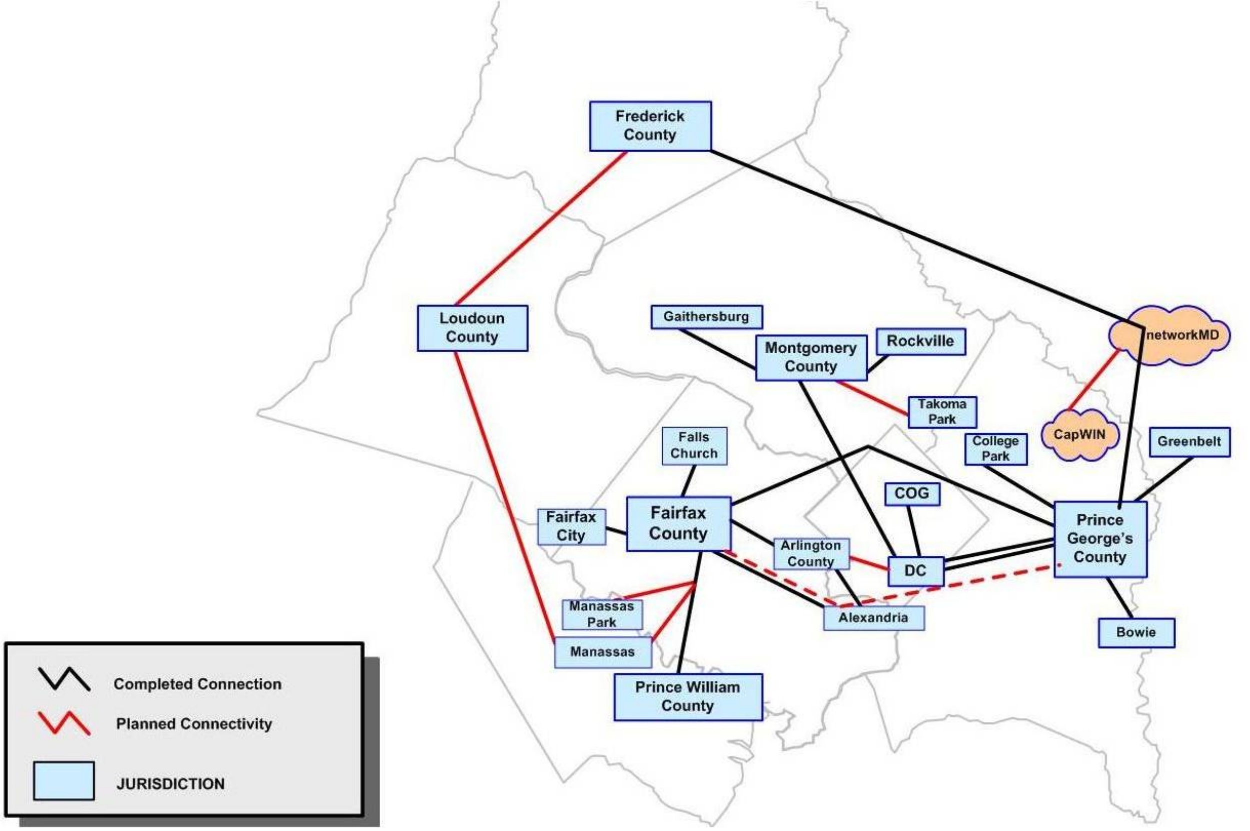
Example NCRnet Site


To Adjacent Interconnection Node
Gigabit Ethernet Link
Ethernet Router / Switch
Extranet Router
Firewall
ESF-5a VTC
Existing Jurisdictional Network
NCRnet
Individual Jurisdiction / NCRnet Participant
Demarcation of responsibility

The NCRnet design provides scalability as application needs expand; allows maximum jurisdictional control and risk management; and ensures the integrity of NCRnet, further simplifying governance.

What Has Been Achieved?

After the first two years of effort, the District of Columbia, Montgomery County, MD, Prince George's County, MD, Rockville, MD, Fairfax County, VA, the City of Fairfax, VA, Falls Church, VA, Prince William County, VA, and the Metropolitan Washington Council of Governments (MWCOG) were connected. A new round of regional funding was secured by the project stakeholders in 2008, and the CIOs and CAOs of the region specifically desired to connect the remaining jurisdictions. Since then Greenbelt, MD, College Park, MD, Bowie, MD, Frederick County, MD, Gaithersburg, MD, Arlington County, VA, and Alexandria, VA have also been connected. By the middle of 2010, the remaining jurisdictions will be connected.



A needs assessment was conducted and demonstrated the need for routine (as well as emergency) use to ensure effective interoperability in the event of emergency.

With that in mind, the region has already developed one key application for the NCR - a regional project designed and implemented utilizing NCRnet: a regional Emergency Management video conferencing system. This program, which is overseen by the emergency managers in the region, interconnects Emergency Operations Centers (EOCs) in 19 jurisdictions and provides a secure, robust solution independent of commercial networks. The video conferencing is used not just by emergency managers; it is regularly used by CIOs and other government officials, enabling better routine communications among jurisdictions. While the application was implemented with leased frame relay lines, it has been cut over to NCRnet as each jurisdiction was connected. The result is that 15 jurisdictions now run this critical application over NCRnet with the remaining transferring transport onto NCRnet as soon as they become connected. This has not only resulted in a drastic increase in video quality, but also signifies substantial cost savings as costly leased lines are replaced by the NCRnet fiber network while ensuring continuity of operations between the emergency managers when the commercial circuits are saturated.

Planned Applications Enable Routine & Emergency Communications

NCRnet is still in its deployment stage, so the stakeholders continue to plan for new applications. Some of them, such as CAD-to-CAD, have been earmarked for funding specifically to be cut over to NCRnet. Others require little effort to cut over and are anticipated in the near future. Among the applications currently proposed are:

- Web-based incident management and alerting system: Delivers customizable messaging boards to emergency managers and first responders with alerts, reports, graphics, and maps.
- Geographic Information Systems (GIS): Maps and tracks geospatial data. Map elements are stored in a variety of formats with different degrees of security attached to different layers.
- Computer Aided Dispatching (CAD): Facilitates dispatch and response for first responders. CAD is integrated with GIS to exchange information on resources and assets, personnel, calls for service, hospital status/availability, transportation resources, and alert notification.
- Data Exchange Hub (DEH): Facilitates the rapid exchange of key emergency resource data using an Enterprise Service Bus. DEH will list defined data elements from contributing data owners and push them to authorized users and applications. A key focus of the DEH is CAD-to-CAD interoperability.
- Regional Automated Fingerprinting Identification System: Enables NCR law enforcement officials to share fingerprints and mug shots.
- Voice Hotline: Interconnects emergency managers and first responders independently of the public switched telephone network for emergency coordination and routine conferences.
- Training: Facilitates secure joint training across jurisdictions without travel or use of public network resources.
- IT Backup and Recovery: Enables jurisdictions to mirror, save, and restore IT resources at facilities outside the jurisdictions.
- General Government, Education Applications & Transportation data: Shares full-motion, high-quality traffic camera feeds and intelligent transportation system resources regionally.