

## COVER PAGE

### TITLE: INTEGRATED NETWORKING TECHNOLOGIES FOR A SURVIVABLE NETWORK

**ABSTRACT:** *The Integrated Networking Technology prototype demonstrates the capability of several emerging networking technologies to operate together seamlessly to enhance the network services targeted for dynamic mobile environments such as those found in the battlefield. The prototype consists of four technologies: 1) Autoconfiguration technology supports autonomous and rapid network deployment and configuration; 2) Self-Managed Virtual Network (SMVN) technology provides virtual networking capabilities for networks which do not natively support these functions; 3) Integrated Mobility Management technology supports session continuity in the presence of node mobility; 4) Assured IP Quality of Service (QoS) technology supports service quality guarantees for mission-critical applications. The prototype is capable of operating over the various types of equipment and protocols to be utilized in battlefield networks. The prototype is designed such that network services and functions are survivable and reconfigurable. In this paper, we describe the four technologies as well as the integrated prototype in the laboratory environment.*

**KEYWORDS:** Ad Hoc, Auto-configuration, Mobility Management, Survivable Network, Quality of service

**Authors:**

Jasmine Chennikara, Telcordia Technologies, RRC-1B221, 1 Telcordia Drive, Piscataway, NJ 08807, 732-699-2958, [jchennik@telcordia.com](mailto:jchennik@telcordia.com)

Ashutosh Dutta, Telcordia Technologies, RRC-1A220, 1 Telcordia Drive, Piscataway, NJ 08807, 732-699-3130, [adutta@research.telcordia.com](mailto:adutta@research.telcordia.com)

Aileen Cheng, Telcordia Technologies, RRC-1A349, 1 Telcordia Drive, Piscataway, NJ 08807, 732-699-2952, [aileen@research.telcordia.com](mailto:aileen@research.telcordia.com)

Dana Chee, Telcordia Technologies, RRC-1H305, 1 Telcordia Drive, Piscataway, NJ 08807, 732-699-3104, [dana@research.telcordia.com](mailto:dana@research.telcordia.com)

Moncef Elaoud, Telcordia Technologies, RRC-1A212, 1 Telcordia Drive, Piscataway, NJ 08807, 732-699-3132, [moncef@research.telcordia.com](mailto:moncef@research.telcordia.com)

Anthony MuAuley, Telcordia Technologies, RRC-1A225, 1 Telcordia Drive, Piscataway, NJ 08807, 732-699-2431, [mcauley@research.telcordia.com](mailto:mcauley@research.telcordia.com)

Isil Sebuktekin, Telcordia Technologies, RRC-1A213, 1 Telcordia Drive, Piscataway, NJ 08807, 732-699-2285, [isil@research.telcordia.com](mailto:isil@research.telcordia.com)

Byung Suk Kim, Telcordia Technologies, RRC-1B225, 1 Telcordia Drive, Piscataway, NJ 08807, 732-699-3152, [bskim@research.telcordia.com](mailto:bskim@research.telcordia.com)

James Burns, Telcordia Technologies, RRC-1K306, 1 Telcordia Drive, Piscataway, NJ 08807, 732-699-3093, [burns@research.telcordia.com](mailto:burns@research.telcordia.com)

Maya Yajnik, Telcordia Technologies, RRC-1C309, 1 Telcordia Drive, Piscataway, NJ 08807, 732-699-2352, [myajnik@research.telcordia.com](mailto:myajnik@research.telcordia.com)

Larry Wong, Telcordia Technologies, RRC-1D309, 1 Telcordia Drive, Piscataway, NJ 08807, 732-699-3164, [larryvw@telcordia.com](mailto:larryvw@telcordia.com)

Ken Young, Telcordia Technologies, RRC-1A329, 1 Telcordia Drive, Piscataway, NJ 08807, 732-699-2221, [kcy@research.telcordia.com](mailto:kcy@research.telcordia.com)

Henning Schulzrinne, Columbia University, 450 Computer Science Building, New York, NY 10027 212-939-7005, [hgs@cs.columbia.edu](mailto:hgs@cs.columbia.edu)

# INTEGRATED NETWORKING TECHNOLOGIES FOR A SURVIVABLE NETWORK

*J. Chennikara, A. Dutta, A. Cheng, D. Chee, M. Elaoud, T. McAuley, I. Sebuktekin, B. Kim, D. Wong, J. Burns, M. Yajnik, L. Wong, K. Young – Telcordia Technologies, Piscataway, NJ, 08854*

*Henning Schulzrinne, Department of Computer Science, Columbia University, NY 10027*

## ABSTRACT

*The Integrated Networking Technology prototype demonstrates the capability of several emerging networking technologies to operate together seamlessly to enhance the network services targeted for dynamic mobile environments such as those found in the battlefield. The prototype consists of four technologies: 1) Autoconfiguration technology supports autonomous and rapid network deployment and configuration; 2) Self-Managed Virtual Network (SMVN) technology provides virtual networking capabilities for networks which do not natively support these functions; 3) Integrated Mobility Management technology supports session continuity in the presence of node mobility; 4) Assured IP Quality of Service (QoS) technology supports service quality guarantees for mission-critical applications.*

*The prototype is capable of operating over the various types of equipment and protocols to be utilized in battlefield networks. The prototype is designed such that network services and functions are survivable and reconfigurable. In this paper, we describe the four technologies as well as the integrated prototype in the laboratory environment.*

## I. INTRODUCTION

The evolution of battlefield scenarios has driven the development of enhanced networking technologies which can survive when communications networks are subject to rapid deployment and configuration. Military networks have a number of network service requirements which differentiate it from the commercial world. Military networks are generally dynamic and mobile as well as survivable in node failure scenarios. Such networks should support a number of routing protocols as well as dynamic and autonomous configuration of IP and virtual networks. Battlefield networks should also handle fast handoff for mobile nodes as well as service quality assurances for mission-critical traffic.

Much work has been done in the commercial world to support basic networking capabilities for fixed and mobile networks. Existing IP configuration mechanisms, such as DHCP, allocate and assign IP addresses but can incur overhead and latency when applied to dynamic

networks. Traditional Mobile IP schemes address node mobility issues but can also incur latency that military survivable networks cannot tolerate. Quality of service in commercial networks generally target fixed nodes with little movement and do not function well in survivable networks. Commercial VPN mechanisms require manual setup which can be time-consuming in the military environment, and does not allow for dynamic association of mobile nodes to VPNs.

We propose a suite of protocols which mitigate the drawbacks found in existing commercial technologies in order to make them more applicable to survivable networks. The prototyped technologies were developed independently to target specific network service issues but have also been integrated to provide a more complete suite of services for survivable networks. The prototype consists of four technologies:

- *AutoConfiguration* technology provides the capability to autonomously configure IP networks for rapid deployment and re-organization.
- *Self-Managed Virtual Network (SMVN)* technology provides multicast and virtual networking capabilities for nodes which do not natively support these functions.
- *Integrated Mobility Management (IMM)* technology supports the ability to ensure that nodes can be located and end-user applications can be provided with continuous session connectivity in the presence of node mobility.
- *Assured IP Quality of Service (QoS)* technology provides the capability to support real-time and non-real-time multimedia traffic (e.g. voice, video, data) on a single network with appropriate service quality guarantees to mission-critical applications.

These technologies are based on enhancements of some standard IETF-based protocols such as SIP and DiffServ, as well as new protocols such as DRCP, MIP-LR and MMP.

The technologies have been developed to work with COTS equipment and protocols as well as military radios. The design is such that as long as there are nodes capable of performing network services, the network can reconfigure itself to maintain and support mobile users,

mission-critical sessions and enhanced functionalities of COTS and military machines.

In this paper, we describe the architecture considerations, interaction among the four network technologies and the results of the prototype in a laboratory environment. Section II describes the network architecture that the technologies target. Section III gives a brief description of each technology and Section IV provides details on the integrated prototype. Section V concludes the paper.

## II. NETWORK ARCHITECTURE

The integrated prototype can be supported over various network architectures and capabilities. The basic requirement for the prototype is that the majority of the nodes in the network should be IP-based. The communications links between nodes can be based on commercial wireline and wireless products, such as 802.3 and 802.11b, or military radios. Figure 1 depicts an architecture which provides both wireless and wireline connectivity for nodes with varying roles in the network. These nodes are either located in terrestrial networks or in airborne nodes. The underlying IP routing protocol is RIP but the prototype has the flexibility to work with other routing mechanisms. The IP nodes in the network form IP subnets by connecting to nodes within communications range that have the appropriate frequency and network IDs. Non-IP based nodes can be part of the network but with limited network services from the integrated technologies suite.

Nodes have the ability to function with one or more network roles. Nodes can be configured to act as servers to manage an enhanced network service designated by the integrated technology prototype or for basic network functions such as DNS. There can also be highly-capable nodes, such as airborne nodes, which enter the network and trigger server functions, residing on other nodes, to migrate to the highly-capable node. Nodes identified as routers will appropriately forward IP packets to one or more destinations, with additional services to enhance forwarding as designated by the integrated technologies protocol suite. Nodes may also behave as mobile host devices which participate in end-user communications. Certain nodes may be configured with privileged network control and access. Such nodes would exist in command and control centers and can manage or control nodes remotely. Any single node can support one or more of the network roles provided that appropriate software, network connectivity and processing power are available.

Within this network architecture, the Integrated Networking prototype handles the following major capabilities:

- Network configuration: Nodes are activated in the battlefield and dynamically assigned IP addresses. Once IP configuration is complete nodes will participate in an election process and nodes with high capabilities will be selected to perform server

functions for specific network services such as QoS, DNS, etc.

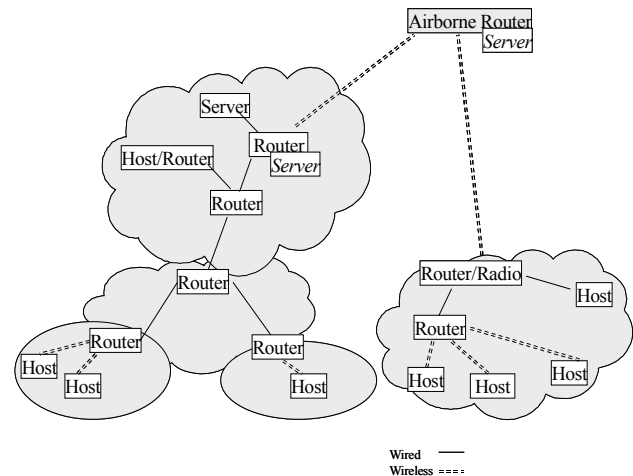


Figure 1. Network Architecture

- Mobility management: Nodes may move within a subnet while participating in an active session. The movement within the subnet may require the node to handoff wireless connectivity from one access point to another within its transmission range. Nodes may also move between subnets in mid-session. Such events require the mobile nodes to receive an IP address update and to notify the corresponding node.
- Quality of Service: Nodes which require ensured service quality for sessions will make requests to the QoS server for allocation of QoS resources. Admitted QoS flows are marked as high priority and the packets are routed through the network with preferential treatment.
- Virtual Networks: Subsets of nodes involved in performing specific tasks or requiring multicast communications will set up a virtual group for the task and communicate over virtual links.

## III. SURVIVABLE NETWORK TECHNOLOGIES OVERVIEW

In this section we discuss the basic components, and design features of each technology. Figure 2 depicts the components of each of the four technologies to be described.

### A. Autoconfiguration

Because of the dynamically and rapidly changing environment inherent within a military network, nodes and routers will be subjected to frequent IP address reconfiguration as well as server reconfiguration. Thus it is essential to keep in place a mechanism whereby rapid robust reconfiguration can readily be applied to the nodes, routers and servers. DRCP (Dynamic and Rapid Configuration Protocol), DCDP (Dynamic Configuration

Distribution Protocol) [9], YAP, and Adaptive Communications Manager (ACM) constitute an IP Autoconfiguration Protocol Suite (IPAS) [10] that help configure the hosts and routers with IP addresses, and other essential servers such as DNS, SIP etc. in dynamic and ad hoc environments.

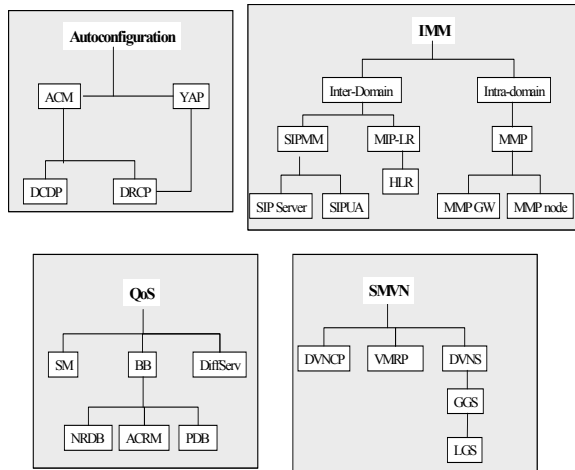


Figure 2. Integrated Prototype Components

DCDP is a robust, scalable, low-overhead, and lightweight protocol designed to distribute configuration information on address pools and other IP configuration information such as DNS server's IP address, security keys, or routing protocol. It operates without central coordination or periodic messages. DCDP also does not rely on a routing protocol to distribute the information.

DCDP relies on the Dynamic and Rapid Configuration Protocol to actually configure the interfaces. DRCP borrows heavily from DHCP but adds features critical to roaming users. DRCP can automatically detect the need to reconfigure through periodic server advertisements. In addition, DRCP also allows for: a) efficient use of scarce wireless bandwidth, b) dynamic addition or deletion of address pools to support server fail-over, c) message exchange without broadcast and d) clients to be routers. From experimental results [10], we observe that it takes up to 5 seconds to configure 80 nodes in a distributed subnet environment where configuration is initiated at a specific root node.

YAP is a simple bandwidth efficient reporting mechanism for dynamic networks. YAP runs on every node and periodically reports its node's capabilities, configuration and operational status. The ACM handles functions such as resetting the network and distributing a new address pool based on human input or from a predefined private address pool.

IPAS protocol suite also provides robustness for server failure. In case of a server failure, ACM together with YAP's reporting mechanism can choose a new node to provide this service and advertises it as the new server through the configuration protocol (e.g., DRCP/DCDP).

This automatic reconfiguration procedure provides a high degree of server survivability than having a set of back-up servers.

IPAS protocol suite meets the rapidly deployable and survivable requirements in a military environment. It configures the network through DCDP and DRCP, reacts to node mobility by reconfiguring the nodes when they move from one subnet to another and reconfigures the DNS, SIP servers without any manual intervention.

### B. Quality of Service (QoS)

The main goal of the QoS technology is to ensure the quality and timely delivery of mission-critical traffic even when the network may experience degradation due to overload and link fluctuations. While absolute guarantees on variable bandwidth lossy wireless networks cannot be made, relative assurances can be provided such that flows classified as high-priority receive preferential treatment in the network [3]. The IP QoS architecture enables support of end-to-end QoS assurances to multiple traffic classes over heterogeneous networks that may encompass wireline and wireless backbones.

The assured IP QoS architecture relies on integration of two complementary approaches:

1. Differentiated Services (DiffServ) [4][5] enables QoS resource management supporting classification, conditioning and marking of traffic flows into service classes. The service classes are virtually segregated and receive class-appropriate differentiated treatment according to specified DiffServ policies and per-hop forwarding behaviors (PHBs).
2. A centralized management entity, called the Bandwidth Broker (BB), provides QoS resource management and admission control of flows into the QoS service classes.

The assured QoS capability involves the host nodes, routers and BBs working collaboratively to adapt the QoS resource management and admission control functions to the underlying networks and defined service classes. The integrated QoS approach, presumes that all network IP routers support DiffServ and enabling technologies for uniform performance guarantees. While lack of DiffServ support does not hinder best-effort IP forwarding, each non-DiffServ router under moderate traffic load would degrade the performance of flows.

The core routers of the network and the edge routers providing access to end-hosts perform DiffServ functions such as conditioning, scheduling and queue management. The DiffServ Code Point (DSCP) field in the IP header provides the classification information used by routers to make packet scheduling and dropping decisions.

The Service Manager (SM), residing on all IP nodes, is used as a proxy application to request, and release, QoS resources from the BB with no modification to the

IP application generating the traffic flow. Commonly, the end-user requests QoS resources for its own application flows, but remote entities such as command and control nodes can also request QoS resources on behalf of end-nodes.

The Bandwidth Broker consists of three functional components:

- *Network Resource Database (NRDB)*: This database maintains topology information in the network such as IP addresses and interfaces per router as well as available bandwidth on each link and subnet. It also maintains QoS information such as active QoS flows and allocated QoS bandwidth.
- *Policy Database (PDB)*: The PDB maintains domain-wide service policy information and flow-specific policies. Domain-wide DiffServ policies, configured at each router, include the description of the service classes supported as well as the per-class scheduling and queue management policies and parameters. Per-flow edge policies define the specific rate and burst control parameters applied to conditioning admitted flows.
- *Admission Control and Resource Manager (ACRM)*: This component performs QoS resource management functions such as DiffServ policies configuration at network initialization time as well as after policy and topology changes. It also handles the flow admission control process.

We have implemented IETF's Expedited Forwarding (EF) and Assured Forwarding (AF) standards [5]. We utilize the EF PHB for network control traffic. Therefore, BB and other network signaling traffic are prioritized over application traffic. The four AF PHBs are used to segregate VoIP, Video/IP, UDP/IP and TCP/IP applications traffic. The three drop-precedence levels within each AF queue enable three grades of service per AF class.

In a typical admission request exchange, the end-host SM sends a QoS admission request to the BB. The BB determines the available capacity for the requested traffic class on the path between the source and the destination. It grants or denies admission into the service class based on available capacity and the QoS requirements. Marking and policing policy based on a multi-field classification of the packet headers are also formulated for individual flows and are configured on the ingress router as part of the admission control process. Flows which are not allocated QoS resources are mapped to Best Effort service class, which has no QoS guarantees.

Without QoS, all network flows compete with each other for network resources such as bandwidth. This often results in degradation of all flows for high network loads and reduction in effective utilization of the network. By using the QoS technology, efficient network utilization as well as bounded loss and delay performance is achieved for real-time as well as non-real-time service classes.

### C. Self-Managed Virtual Network (SMVN)

We developed an application-level solution Self-Managed Virtual Networks (SMVN) [1] to provide enhanced features similar to IP-based Virtual Private Networks (VPN), interconnecting neighbors using virtual links. The SMVN capabilities are built in the application layer rather than the network layer to mitigate routing protocol complexity, and scalability restrictions. SMVN creates an information-centric networking environment on top of an existing IP network, to more readily support applications which will communicate among geographically diverse nodes with similar services. Our SMVN approach provides an efficient virtual networking through built-in self-configuring mechanisms under dynamic networking environments where stationary and mobile nodes coexist, without the need for human intervention even under severe networking conditions.

SMVN consists of a suite of protocols including Dynamic Virtual Network Configuration Protocol (DVNCP) [1] for virtual network formation and maintenance as well as the Virtual Mesh Routing Protocol (VMRP) [2] for route management within the SMVN.

SMVNs are created and maintained through the use of the DVNCP protocol which takes advantage of the hierarchical architecture of Domain Virtual Network Servers (DVNS), Global Group Servers (GGs) and Local Group Servers (LGS) to track members belonging to any SMVN. The DVNS maintains a database of all virtual network servers. Each SMVN has a GGS maintaining a database of all the LGSs for the SMVN. The LGS is a database local to a domain that contains a comprehensive list of all members in the domain. In addition, the LGS receives a sample list of member nodes outside its domain to support inter-domain connectivity of SMVN nodes.

To join a particular SMVN, a node contacts the DVNS server to learn about SMVNs in the area. The DVNS responds with the IP address of the LGS, if available, or the GGS if an LGS is not available in the domain. The new node obtains a list of current members from the SMVN server (LGS or GGS). Based on the listing, the new node contacts some (or all) of the advertised nodes and establishes virtual connections to the virtual neighbors using DVNCP. DVNCP will also periodically provide updated information on the virtual connection and virtual neighbor status.

Unicast and multicast routing is accomplished with Virtual Mesh Routing Protocol (VMRP). VMRP routing is based on the SMVN virtual topology and is designed to provide every SMVN node with knowledge of the topology of the entire SMVN. VMRP takes advantage of the DVNCP capabilities to derive local neighbor topology information and virtual link cost information for routing purposes. Local SMVN neighbor information is exchanged and updated among SMVN nodes in order to build and maintain the entire SMVN topology information at each node. The distribution of the routing

information is performed through a spanning tree which includes all the members of the SMVN. The spanning tree branches are added/removed as new members join/leave the SMVN. With the routing information distributed via the VMRP spanning tree, each node can make independent calculations on shortest path routes to SMVN members.

Packets exchanged among SMVN members may physically pass through multiple non-member nodes. However, since there is an underlying mesh of virtual connections, packets may be sent over any transport protocol (e.g., TCP or UDP) and any network protocol (e.g., IP unicast, IP multicast, or IPSec). In addition, the presence of non-SMVN nodes in the network does not compromise the functionality of SMVNs.

SMVNs are designed to handle multicast applications. We assume that for any SMVN, multicast applications will require distribution to all the nodes which are part of an SMVN, i.e., broadcast within the SMVN. If IP multicast is available we can use it for these purposes. However, IP multicast is not required by the SMVN because VMRP provides a structure for the distribution of multicast packets which is independent of the IP capabilities. Similar to other multicast algorithms, we use a single shared tree to distribute data. VMRP does not use a core node to be the point of distribution for multicast packets as in PIM but instead allows any source node to distribute directly over a single tree in order to limit tree maintenance overhead. The VMRP spanning tree used for topology distribution also functions as the tree for distribution of multicast packets.

We developed SMVN as a technology to provide selective bypass routing, without affecting the underlying IP routing protocols. In addition, the SMVN approach is transparent to the changes in the underlying physical network. This solution exploits the plug-and-play and robust self-healing virtual network infrastructure as well as providing a means to support multicast capabilities when native IP multicast is not available.

#### *D. Integrated Mobility Management (IMM)*

The Integrated Mobility Management (IMM) [6][7] technology supports seamless session continuity for mobile nodes in the battlefield network. Mobile nodes may participate in sessions with corresponding hosts (CHs) while connected to the network via a particular access point. However, as the node moves, the initial access point signal strength may not be sufficient to maintain the connection. The mobile node then connects to the network via a different access point which may be within the same domain or in another domain. The IMM technology allows nodes to maintain their session with CH despite location changes.

In designing the IMM technology, we considered the drawbacks of traditional Mobile IP. Mobile IP (MIP) is the standard scheme for IP mobility management. MIP has several strengths, including transparency to upper layers and no required modifications at the CH.

However, basic MIP has some shortcomings which IMM is designed to avoid. MIP routing through the Home Agent, known as triangular routing, is inefficient. MIP signaling introduces handoff latency in addition to the latency incurred at the link and physical layers. MIP registration signaling and encapsulation also incur overhead. The basic MIP scheme does not work with network firewalls which filter packets based on source address. In addition, MIP has limited survivability since the Home Agent, if unavailable to route packets to mobile nodes, becomes a single point of failure.

The IMM [6][7] technology consists of components to support both real-time and non-real-time traffic with node mobility within and between domains. We designed the Micro-Mobility Management Protocol (MMP), to handle micro-mobility, i.e. node mobility within a domain, for both real-time and non-real-time traffic. For macro-mobility, i.e. node mobility between domains, we use the Session Initiation Protocol-based Mobility Management (SIP-MM) to handle node mobility for real-time traffic and Mobile IP with Location Registers (MIP-LR) to handle mobility for non-real-time traffic.

Although MIP-LR alone can handle both real-time and non-real-time traffic, we use it only for non-real-time traffic. We use SIP-MM for macro-mobility for real-time-traffic because: (a) SIP [8] is already used for session control signaling for real-time applications, and mobility can be handled using the same signaling mechanisms; (b) SIP handling of terminal mobility integrates well with SIP personal mobility (employing a unique URI for the user); and (c) a SIP-based solution exists for smooth handoffs of real-time traffic streams. In order, to use both SIP-MM and MIP-LR for macro-mobility management, we use a policy table so that real-time packets are captured only by the SIP-MM component and the non-real-time packets by the MIP-LR component.

SIP-MM handles mobility scenarios where mobile nodes, with on-going sessions, change to access points which are in different domains or subnetworks. SIP User Agents (SIPUAs) reside on the mobile nodes to support SIP functions and SIP servers reside in the domain. A mobile node uses SIP INVITE messages to initiate sessions. SIP-based terminal mobility using re-INVITE messages to the CH then provides fast handoff for real-time multimedia traffic as the mobile nodes moves from one subnet to another. As a mobile node changes subnet, the node's IP address changes, via autoconfiguration protocols, to provide IP connectivity within the new subnet.

For non-real-time traffic, IMM uses MIP-LR which reduces MIP forwarding and provides profile replication. In MIP-LR, the database mapping of the mobile node's IP address to its care-of address is maintained by a Home Location Register (HLR). The HLR query in MIP-LR for mobile node location is similar to the HLR query in cellular systems. Unlike the Home Agent, HLR need not be located in the home network, and can be replicated for

survivability and redundancy, as often needed in military networks.

For mobility of nodes within the same subnet, i.e., requiring no IP address update, we use MMP. The Micro-Mobility Management Protocol (MMP) is an extension of Cellular IP suitable for ad hoc networks, where the nodes and gateways are dynamically configured using mechanisms such as the autoconfiguration technology. MMP nodes are the access point nodes, discovered via beacons, providing connectivity into the network for the mobile node. The MMP gateway is a node which tracks mobile nodes via their connectivity to MMP nodes. The MMP gateway provides mobility support when the mobile node moves within a domain, by using host-based routing internal to the domain. Upon network configuration, the mobile node sends an update, including its IP address, to the MMP gateway. The IP address is stored and the host-based route cached along the path to the gateway. When handoffs occur within a domain, route caches are updated, so handoff latency is at most the time it takes for the update to reach the MMP gateway within the domain. Thus compared to inter-domain handoff, intra-domain handoff occurs with very low handoff delay.

In a typical scenario, as a mobile node moves within a domain, it may connect to different MMP nodes, choosing the best MMP node based on the strength of the MMP beacons heard by the mobile node. When the mobile node moves into a different domain, it will connect to the local MMP node and also autoconfigures to obtain a new IP address. The mobile node then updates the new local MMP gateway with its IP address and route. It then sends a SIP re-INVITE message to the CH with the new IP address to maintain the real-time traffic and sends a MIP-LR update to maintain the non-real-time traffic. Thus SIP-MM and MIP-LR interact with MMP to support inter- and intra-domain mobility.

#### IV. INTEGRATED PROTOTYPE

In the integrated testbed, we support integrated network configuration, mobility management, quality of service control and virtual networking capabilities. The details of the testbed are depicted in Figure 3.

All the routers and nodes under our control use the Linux 2.4.7 kernel with iptables and advanced routing and traffic control (tc) modules enabled for DiffServ capability. All other prototype software was developed in user space.

In the network we use RIP for the wired network, with IMM to support node mobility. We define the network on the left side of the R4 node as the backbone network. On the right side of R4, are two remote networks, named R2 and R3 remote nets. R4 is a router/server node that may periodically or temporarily join the network, providing connectivity between the backbone network and the remote networks.

For this testbed, we describe a sample scenario which shows the integration among the four technologies.

Initially, the R1 router initiates the autoconfiguration of the backbone network. Note that the mobile1 node initially is connected via the MMP Node1 (location 1) and receives an appropriate IP address for that MMP Node1 subnet. R4 is not connected thus the remote networks are not configured yet. Through network server selection, R1 is designated as BB, DVNS, YAP, ACM, etc. and this information is advertised to all nodes.

When R4 is connected to the backbone network, the R4 router as well as the R3 and R2 networks are configured via DRCP/DCDP. The autoconfiguration protocol then migrates the BB and DVNS functions to R4 because it is advertised as a high capability node for supporting these functions. The autoconfiguration protocol provides a GUI for user viewing of the final network topology configuration, subnet grouping, IP addressing and server nodes.

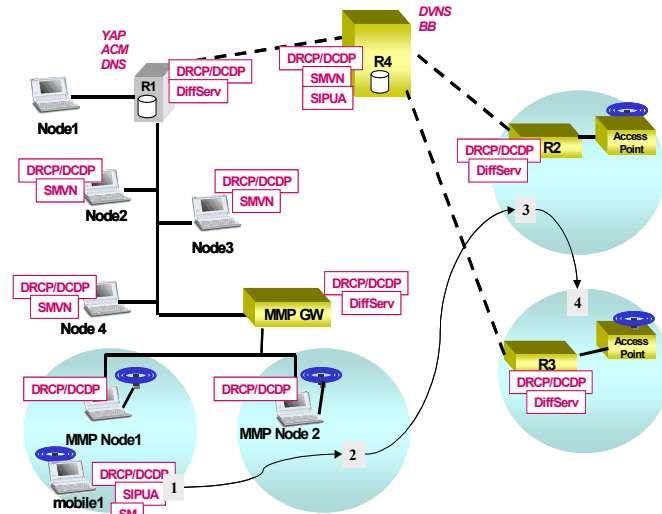


Figure 3. Prototype Testbed

After configuration, R4, Node2, Node3 and Node4 dynamically form an SMVN mesh to receive video. The mobile1 node user initiates a SIP video session to R4. R4 acts as a video source to the backbone network and multicasts the video stream to the nodes in its SMVN network.

While sending video to R4 the mobile1 node moves within the subnet and attaches to MMP Node2 (location 2) via the MMP protocol. The SIP video session to R4 and the SMVN nodes is maintained.

The mobile node then moves to the R2 subnet (location 3). After the move into the R2 network, the mobile node gets a new IP address via DRCP/DCDP and the network topology GUI will reflect this update. This time, the mobile node uses the SIP-MM protocol to maintain the video session with the SMVN.

At this point, suppose Node1 begins injecting traffic in the network causing the backbone network links to congest. As a result, the video seen by the SMVN nodes, sent from the mobile node, degrades. The mobile node then makes a request to the BB to admit the video stream to the SMVN as a prioritized traffic flow. The request is

accepted using the topology information that BB obtains from the YAP Server. QoS resource management is performed and the video stream quality improves even though the network is congested by best effort traffic from Node1.

The mobile node makes one last move to the R3 network (Location 4) using SIP-MM to support mobility. The mobile node receives a new IP address from DRCP/DCDP. The BB receives the new IP address update and accordingly updates its resource allocation and flow information so that QoS to the video flow is maintained even with mobility.

Table 1 shows some of the performance figures obtained from the prototype testbed using the integrated networking technologies. We considered the configuration times for IP networks and virtual networks. Using DRCP/DCDP, the autoconfiguration time for a specific client in a single subnet is limited to 500 ms, but it takes up to 5 seconds to configure about 80 nodes in a distributed network. For SMVN, the configuration time, including virtual link creation time, in an 8-node network is close to 1 second.

For IMM, the packet loss due to handoff is minimum during micro-mobility. This is a result of MMP's smooth handoff feature. Packet drops due to macro and domain handoff is dependent upon both the mobile node's IP configuration time as well as SIP Re-INVITE or MIP-LR update latency. Note that the IMM configuration time is the initial IP network configuration time via autoconfiguration.

For QoS, admission control and resource allocation for a new flow takes about 21 seconds. In addition, for QoS flows of mobile nodes, the time to update topology as well as release and re-allocate QoS resources for the flow is about 32 seconds. In general, higher latencies can be expected when the inherent link characteristics introduce packet loss and degradation. This becomes more probable when using legacy radios.

**Table 1: Performance Summary**

Technology	Configuration Time	Update Latency (Handoff)	Packet Loss
IMM	~ 500 ms	Macro ~ 400 ms Micro ~ 100 ms Domain ~ 600 ms	Macro: 50 pkts/handoff Micro: 1 pkts/handoff Domain: 60 pkts/handoff
SMVN	Tunnel setup ~ 740 ms Routing setup ~ 210 ms	N/A	N/A
QoS	Request ~ 21 sec Delete ~ 3 sec	Update ~ 32 sec	Affected by link characteristics
Auto-configuration	Linear ~ 6-16 sec Distributed ~ 4-5 sec Single subnet ~ 500 ms	N/A	N/A

## V. CONCLUSIONS

The Integrated Networking Technology prototype demonstrates the capabilities of several emerging

networking technologies: Autoconfiguration, SMVN, QoS and IMM. The networking technologies were designed to meet the overall objectives of reconfigurability and survivability of military networks.

We have developed a system which leverages the capabilities of each technology in an integrated network environment to limit unnecessary duplication of network information and maintain communication with essential network services. For example, the autoconfiguration technology supports dynamic election of network servers including those used by the assured IP QoS and SMVN technologies as well as the handoff of these network servers between networks/nodes. Mobility management and autoconfiguration protocols also interoperate to maintain valid IP addresses and network information for mobile nodes. We leverage network topology information provided by the autoconfiguration databases to support the resource reservation functions of the IP QoS technology. The IP QoS technologies also provide QoS guarantees to SMVN and IMM signaling traffic. Additionally, the IMM technology interacts with IP QoS to maintain session quality for mobile users.

We continue to enhance some of these technologies for value-added services in response to specific networking requirements such as highly mobile ad hoc networks, information assurance, integration with legacy radios, etc.

## REFERENCES

- [1] M. Elaoud, G. Kim, A. McAuley and J. Chennikara, "Self-Managed Virtual Network (SMVN) for Enhancing Military Network Capabilities," *IEEE Military Communications Conference*, Maclean, USA, October 2001.
- [2] J. Chennikara, M. Elaoud, G. Kim, and A. McAuley, "Enhanced Routing for Military Self-Managed Virtual Networks," *IEEE Military Communications Conference*, Maclean, USA, October 2001.
- [3] B. Kim, I. Sebuktekin, "An Integrated IP QoS Architecture - Performance," *IEEE MILCOM*, Los Angeles, CA, October 2002.
- [4] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss, "An Architecture for Differentiated Services," *IETF RFC 2475*, December 1998.
- [5] K. Nichols, B. Carpenter, "Definition of Differentiated Services Per Domain Behaviors and Rules for their Specification," *IETF RFC 3086*, April 2001.
- [6] A. Dutta, R. Jain, K. D. Wong, J. Burns, K. Young, H. Schulzrinne, "Multilayered Mobility Management for Survivable Network," *IEEE Military Communications Conference*, Maclean, USA, October 2001.
- [7] K. D. Wong, A. Dutta, J. Burns, R. Jain, K. Young, H. Schulzrinne, "A Multilayered Mobility Management Scheme for Autoconfigured Wireless Networks," *IEEE Wireless Communications Magazine*, October 2003.
- [8] H. Schulzrinne and E. Wedlund, "Application-Layer Mobility using SIP," *Mobile Computing and Communications Review (MC2R)*, July 2000.
- [9] A. McAuley, A. Misra, L. Wong et al, "Experience with Autoconfiguring a Network with IP addresses," *IEEE MILCOM*, October 2001.
- [10] A. McAuley, D. Chee et al., "Automatic Configuration and Reconfiguration in Dynamic Networks," *Army Science Conference*, December 2002.