FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone: +46 8 555 030 00
Fax: +46 8 555 031 00

www.foi.se

Routing Aspects on Soldier Node System

JIMMI GRÖNKVIST, ANDERS HANSSON AND MATTIAS SKÖLD

FOI-R--3642--SE
ISSN 1650-1942

February 2013

Jimmi Grönkvist, Anders Hansson and Mattias Sköld

Routing Aspects on Soldier Node System

Titel	Routingaspekter för Buret Krypto
Title	Routing Aspects on Soldier Node System
Rapportnr/Report no	FOI-R--3642--SE
Månad/Month	Februari/February
Utgivningsår/Year	2013
Antal sidor/Pages	27
ISSN	1650-1942
Kund/Customer	FMV
FoT område	Ledning och MSI
Forskningsområde	Kommunikation och IT-säkerhet
Projektnr/Project no	E32306
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Avdelningen för Informations- och aerosystem

Sammanfattning

Buret Krypto (”Soldier Node” på engelska) ska ge enskilda soldater förmåga att kryptera/dekryptera tal och data i en taktisk miljö. Som förberedelse för en upphandling är det viktigt att undersöka om det finns möjliga tekniska lösningar som uppfyller Försvarsmaktens ställda krav. Syftet med rapporten är att undersöka konsekvenserna av olika routing-alternativ i Buret Krypto.

För att utvärdera olika routing-alternativ har vi definierat fem nätspecifika användningsfall baserade på Försvarmaktens krav på Buret Krypto. Följande tre routing-alternativ beaktas: (*Host*) Buret Krypto uppträder på ett liknande sätt som en vanlig bärbar dator ansluten till ett datornät via ett Ethernet-gränssnitt. (*Dual host*) Buret Krypto beter sig som två olika värdar sett från IP-nätverket. Beroende på vilka gränssnitt som är aktiva så växlar Buret Krypto internt mellan förkonfigurerade statiska routingtabeller. (*Router*) Buret Krypto innehåller en router som kör dynamiska routingprotokoll på alla gränssnitt.

Eftersom Ra1570 saknar fullt stöd för dynamiska nät, är det oklart om alla användningsfall kan hanteras med Ra1570. En *host*-lösning uppfyller inte kraven på Buret Krypto. Vi visar att med tillräcklig förkonfiguration, kan en *dual host*-lösning hantera de användningsfall som beskrivs i rapporten, men har vissa begränsningar, bl.a. när det gäller unicast-trafik. En *router*-lösning i Buret Krypto har flera attraktiva fördelar såsom: (1) effektiva rutter, (2) applikationens IP-adress är oberoende av mobilitet och (3) kompatibilitet med kommersiella routrar i nätverket. Det är dock oklart om det är möjligt att anskaffa en kommersiell router inom den aktuella tidsramen för Buret Krypto, givet de hårda kraven på fysisk storlek och energiåtgång. Dessutom är det osäkert om mängden administrativ routingtrafik kan reduceras tillräckligt för att användas i ett mobilt radionät. En icke-kommersiell router som är särskilt utformad för låg overhead i taktiska miljöer minskar inte den totala overheaden i ett system som redan har kommersiella routrar.

Nyckelord: Buret Krypto, Soldier Node, routing, multicast

Summary

The Soldier Node, known as “Buret Krypto” in Swedish, will enable individual soldiers to encrypt/decrypt voice and data in a tactical environment. As a preparation for the procurement, it is important to check whether technical solutions exist that fulfill the requirements from the Swedish Armed Forces. The purpose of the report is to examine the consequences of different routing options in Soldier Node.

To evaluate different routing options we have defined five network-specific use cases based on FM requirements on Soldier Node. The following three routing options are considered: (*Host*) The Soldier Node behaves in a similar way as a regular laptop connected to a network with an Ethernet interface; (*Dual host*) The Soldier Node behaves as two different hosts as seen from the IP network. It switches internally between preconfigured static routing tables depending on which interfaces are active; and (*Router*) The Soldier Node contains a router that runs dynamic routing protocols on all its interfaces.

As Ra1570 does not fully support dynamical networks, it is not clear if all use cases are handled with Ra1570. A *host* solution does not fulfill the requirements on Soldier Node. We show that with sufficient preconfiguration, a *dual host* solution can handle all of the use cases described in the report, but has certain limitations, e.g., regarding unicast traffic. A *router* solution in Soldier Node has some attractive benefits, including: (1) routes are efficient, (2) the application IP address is independent of mobility, and (3) compatibility with other commercial routers in the network is good. It is, however, unclear whether a commercial router can be procured within the current time frame of Soldier Node, due to the restrictions on physical size and power consumption. Furthermore, it is not clear today whether the amount of administrative routing traffic can be sufficiently reduced to be feasible on a typical tactical mobile radio network. A non-commercial router, designed for low overhead in tactical environments, does not reduce the total overhead in a system that already has commercial routers.

Keywords: Soldier Node, routing, multicast, encryption

Table of Contents

1 Introduction

The Soldier Node system, known as “Buret Krypto” in Swedish, will enable individual soldiers to encrypt/decrypt voice and data in a tactical environment, see the Request for Information for Soldier Node [1]. It will also act as a simple communications router connecting the following external devices: Headset (clear text audio in, analog), Data in (clear text data, digital), Radio 1 (encrypted data, digital), Radio 2 (encrypted data, digital), Radio 3 (clear text audio out, analog), and Military Vehicle LAN (digital, VoIP/IP), see Figure 1.

The Solider Node will allow the soldier to simultaneously decrypt and listen to all incoming voice channels and encrypt/decrypt data to be sent to a connected soldier computer. Using an internal and/or wireless external PTT selector (Push-To-Talk), the soldier can choose the recipient voice group. To facilitate handling of the Soldier Node in an uncontrolled environment, all personal settings, configuration data and crypto keys are stored on a personal “ignition key” device.

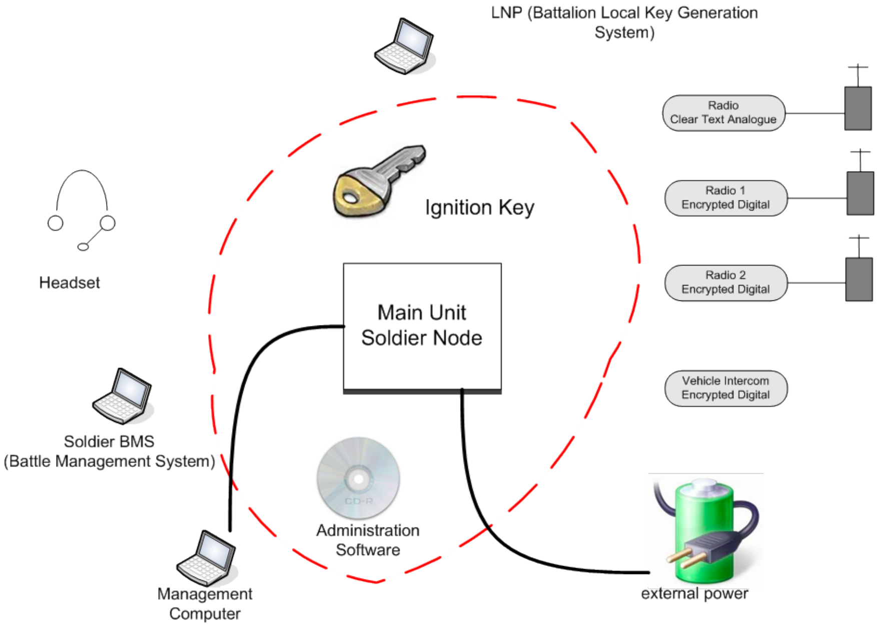
LNP (Battalion Local Key Generation System)
Radio Clear Text Analogue
Radio 1 Encrypted Digital
Radio 2 Encrypted Digital
Vehicle Intercom Encrypted Digital
Ignition Key
Headset
Main Unit Soldier Node
Soldier BMS (Battle Management System)
CD-R
Administration Software
Management Computer
external power

Figure 1: The Soldier Node System.

The soldier is equipped with one handheld radio (radio 1) for communication within the squad, one Soldier Node, one soldier computer (a personal Battle Management System), one GPS, and one headset. Voice communications, position and data from the soldier computer are considered as classified at the Restricted level. Soldier Node will allow the squad members to communicate with each other, listen to commands given by the squad leader, and exchange position information, all in a secure manner.

A squad leader will use the Soldier Node in the same way, but with the addition of an extra radio (radio 2). Radio 2 can be for communicating within the platoon or for long-range communication.

When the squad is inside a vehicle, some of the squad members will be connected to the vehicle LAN via a direct cable. For these, communication with the vehicle crew and with the platoon leader will be routed through the vehicle LAN. The router in the vehicle (KomNod) handles further routing of the encrypted voice and data.

The soldier can be equipped with an additional radio (radio clear text analog in Figure 1), used for unclassified voice only. This allows monitoring of civilian radio communications.

The primary purpose of this report is to discuss the routing functionality in Soldier Node and the consequences of different routing choices for procurement and user experience.

In current tactical radio systems, voice traffic is received separately on an analog interface to the radio, and its processing can be optimized by the radio system. Encrypted voice traffic, on the other hand, is transmitted in data packets, potentially with QoS (Quality of Service) parameters set in the header. The consequences of radio systems that are incapable of reading QoS information are not considered.

In Chapter 2 we first discuss the most relevant requirements of the Soldier Node as seen from routing perspective. Based on these requirements and on discussions with the Swedish Armed Forces, Chapter 3 describes a number of use cases that illustrate the routing problems for Soldier Node. In Chapter 4 we describe different options for Soldier Node routing and discuss their pros and cons through fulfillment of the use cases in Chapter 3. Finally we conclude the report in Chapter 5.

2 Important requirements

The TTEM [2] for Soldier Node puts a large number of requirements on the functionality of the Soldier Node. However, from a routing point of view only a limited number of these requirements are relevant. Through discussions with the Swedish Armed Forces, we have attempted to transform such requirements to technical requirements and use cases from which the routing problem can be analyzed. In general, requirements in the following areas have a large impact on the routing functionality of the Soldier Node:

- Weight and battery time: Limited weight, combined with requirements of long battery time, in difficult environments (especially for cold temperatures) limit the computational ability of the Soldier Node.
- The ability to listen to 2 -3 simultaneous voice groups received on different radios.
- Voice and data at the same time: A user should be able to speak over one radio while simultaneously sending position information on the other radio. This means that traffic must be routed by the Soldier Node.
- Users directly attached to the vehicle LAN should in most cases automatically communicate through the vehicle’s radios, not their own handheld radio.

In addition to these requirements, there are also the requirements that Soldier Node should be able to use Ra 1570 (Harris RF-7800S) [3] and Ra 1512 (Harris RF-5800H-MP) [4]. These radios have certain specific properties that complicate the routing problem. In the rest of the report, we discuss general solutions first, which assumes simpler layer 2 radios. This is done to achieve good compatibility with future systems and thereby avoid a tailored solution to these specific radios. We also discuss how to modify a general solution as little as possible for Ra 1570. For Ra1512 the main challenge is its low capacity so that special solutions, such as recording voice messages, may be required when using external crypto devices. A separate routing solution is probably required for this radio. This is outside the scope of the report.

3 Use cases

In this chapter, we describe a number of use cases that are relevant to routing functionality in Soldier Node (SN). The use cases are based on the requirements described in the previous chapter and discussions with the Armed Forces.

In these use cases, we assume that there are vehicle versions of both the squad radio and the platoon radio. In addition, the vehicle may have other radios as well, such as Ra460 and Satellite Communication. So far very few vehicle versions of the squad radio Ra1032 (Selex PRR) [5] have been procured. It is not expected to be used in many vehicles, but it is included in some of the use cases. In each of these we also discuss what happens if it is not present.

In the different use cases, we number each squad with integers 1 to 5, and each SN is numbered with squad number and individual number, e.g. SN1.5 is SN number 5 in squad 1.

3.1 Use Case 1: Squad moving in and out of its vehicle

Some versions of the squad radio will be installed in a vehicle. This use case is the simplest example that requires routing updates when the user connects to the vehicle LAN.

The first use case describes soldiers communicating within their own squad; this should be possible both as mounted and as dismounted, which can be seen in Figure 2. A squad member is able to communicate with its own squad members both inside and outside the vehicle. When entering the vehicle, connection to the vehicle LAN is simply by attaching a cable to the Soldier Node.

Traffic within the squad is assumed to be primarily multicast to the entire squad. Squad leader and backup squad leader are assumed to have two active radios connected to soldier node.

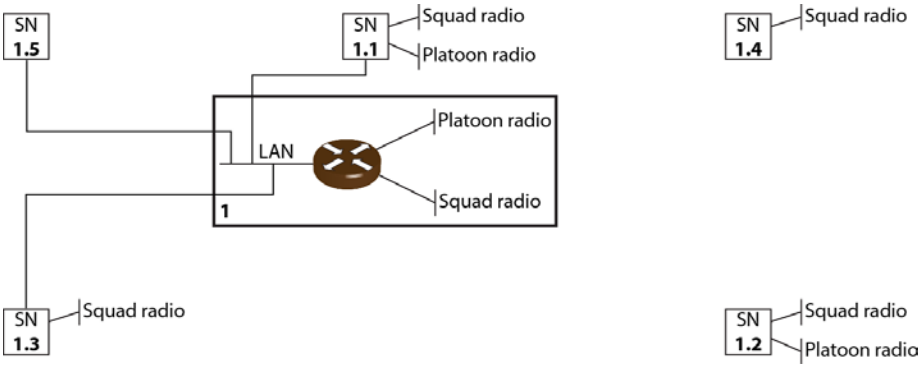

Figure 2: Squad 1 partially inside its vehicle.

When the squad member is dismounted, all voice and data are sent through his squad radio; when the squad member connects to the vehicle LAN, all voice and data is sent on the LAN. Voice and data can be further transmitted by the vehicle's squad radio if some members are not connected to the vehicle LAN.

If no vehicle squad radio is installed in the vehicle, the SN still transmits all voice and data to the squad on his squad radio even when connected to the LAN.

3.2 Use Case 2: Platoon including multiple vehicles and more than one squad

The second use case treats internal platoon communication, which can be seen in Figure 3. This includes multiple vehicles and many users with dual radio interfaces. Using a PTT button, a member of the platoon network should be able to speak to all members of the platoon networks regardless of whether that user is mounted or dismounted and regardless of how many other members are mounted or dismounted.

Normal members of the platoon network are the squad leaders, their backup squad leaders, platoon leaders and vehicle commanders.

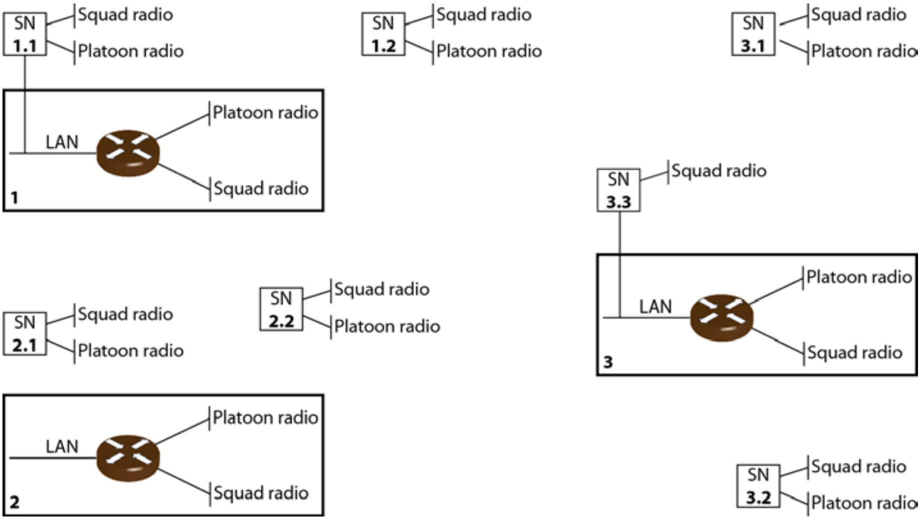

Figure 3: Platoon communication

When the squad leader is dismounted, all voice and data to the platoon network are sent through the platoon radio and all voice and data to the squad are sent through the squad radio. When the squad leader connects to the vehicle LAN, all voice and data are sent on the LAN. Voice and data to the platoon network are routed by the vehicle router to the vehicle platoon radio. Voice and data to the squad are routed by the vehicle router to the vehicle squad radio.

If no vehicle squad radio is installed in the vehicle, the SN transmits all voice and data to the squad on his squad radio even when connected to the LAN.

3.3 Use Case 3: Autonomous platoon and squads

In this case, the radio network is autonomous and is not connected to the IP routers in the vehicles, which can be seen in Figure 4. In general, we have the same assumptions as in the previous two examples. From the squad leader, all voice and data to the platoon network are sent through the platoon radio, and all voice and data to the squad are sent through the squad radio.

This use case requires that the SN system be able to function autonomously without interaction with the vehicle router.

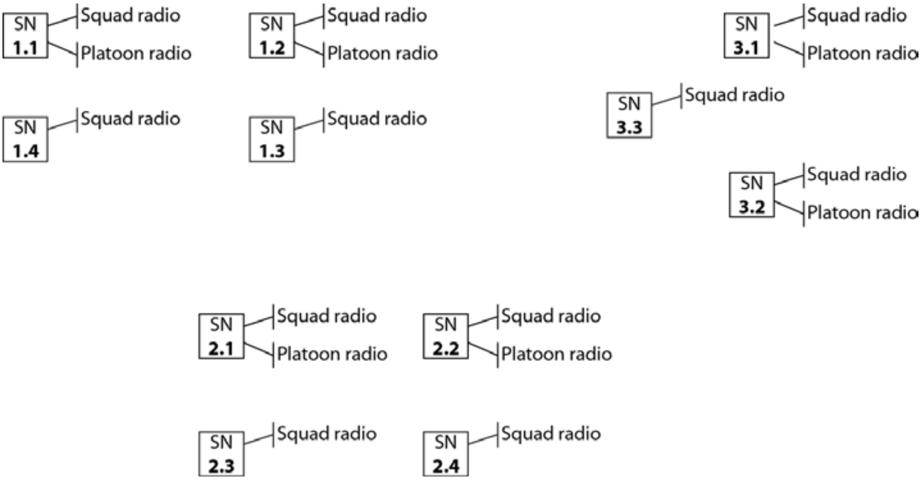

Figure 4: Autonomous networks

3.4 Use Case 4: Switching of group membership

In this use case, some soldiers change their squad membership. We assume a complete switch from one squad to another. This is done in a manner comparable to the switching of frequency of an analog radio. All changes of internal parameters (routing tables, IP addresses or used keys) are invisible to the user.

In Figure 5, SN 2.1 and SN3.1 change membership from squad 2 and 3 to squad 1. This is a user-initiated change of squad radio parameters (such as frequency, transec settings, etc.) as well as a change of the SN’s parameter setting from one preconfigured setting to another preconfigured.

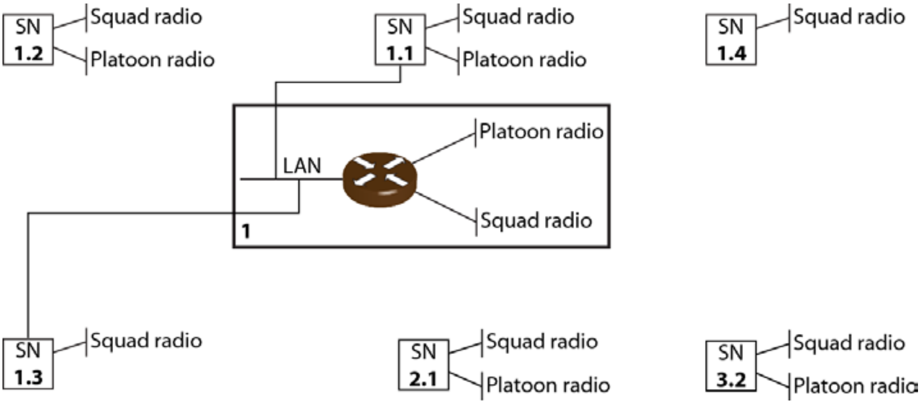

Figure 5: Change of squad membership

3.5 Use Case 5: Company network extension

Here we extend the company network to dismounted units. We assume that one platoon leader is inside a vehicle and equipped with SN X. Furthermore, another platoon leader and a company leader dismount from their vehicles and are equipped with SN Y and SN Z, respectively, see Figure 6. When the company leader is inside the vehicle, all normal communication within the company is sent on the vehicle LAN and is routed by the vehicle router to the vehicle company radio, such as Ra460. When the company leader dismounts from the vehicle, he uses a handheld platoon radio to transmit traffic to the company network. When this traffic reaches the vehicle, it is rerouted by the vehicle router to the company radio and to other users on the vehicle LAN. Whenever the vehicle router receives traffic from the company radio, it retransmits this on its platoon radio to reach the dismounted company leader. Such traffic is sent only to dismounted members, however.

In this use case, it is possible to preconfigure communication groups that are subsets of the company network group (e.g. the company leader and two platoon leaders). Information sent to these groups is only received by its members. However, if many such groups are required, it is probably better to use telephony services using the Session Initiation Protocol (SIP) [7] which can set up less preplanned conversations. This would, however, include more functionality than routing, which is not the primary focus of this report.

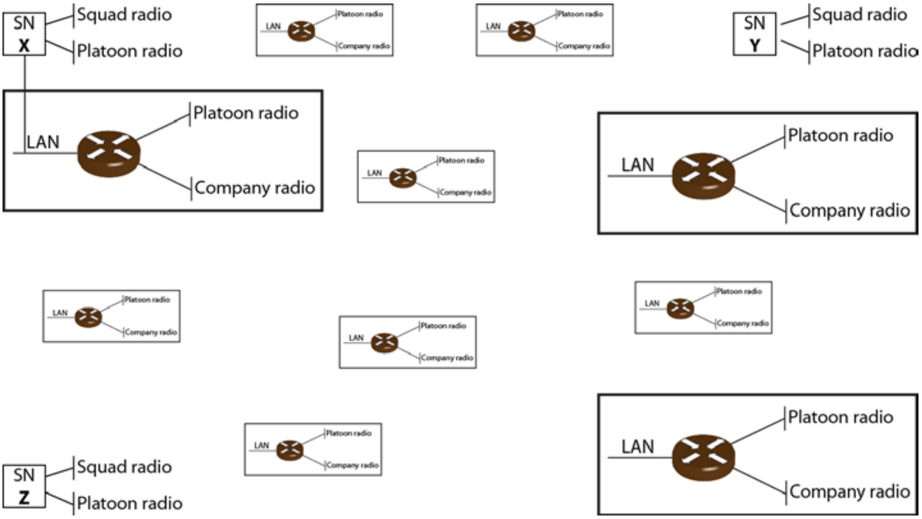

Figure 6: Extension of the company network

4 Routing principles

In this chapter we consider three different principles for the routing functionality in the Soldier Node (SN):

- *Host*—The SN behaves in a similar way as a regular laptop connected to a network with an Ethernet interface.
- *Dual host*—The SN behaves as two different hosts as seen from the IP network. To control how the traffic is routed, it internally switches between preconfigured static routing tables depending on which interfaces are active.
- *Router* —The SN contains a router that runs dynamic routing protocols on all its interfaces.

The first of these principles (*host*) is the most straightforward solution. It is a standard method for connecting to a network and minimizes computation costs, which is advantageous with respect to battery times. However, as it would only allow connection to a single network at a time, this solution does not fulfill even the most relevant requirements in Chapter 2. We discuss the *dual host* principle further in Section 4.1. A solution based on the *router* principle is the most complete solution. In theory it should be able to handle all cases, but at a cost of more overhead in the networks and higher power consumption. It can be divided into two different cases depending on how such a router is implemented. One solution is to use a similar type of router as the vehicle router (KomNod), i.e. a commercial Cisco router, in Soldier Node. The other alternative is to use a router that is compatible to the vehicle router but can also use other protocols. We discuss both of these alternatives in Sections 4.2 and 4.3, respectively.

4.1 Dual host principle

In this type of solution, the SN is viewed as two (or more) separate hosts as seen from the black IP network. This means that the vehicle router, which potentially could reach the SN on two different paths, e.g. platoon radio and squad radio, instead sees two different hosts with two different IP addresses. If for some reason one of these radios fails, no application traffic over the broken path would be deliverable on the other one either.

Internally, the SN automatically switches between two preconfigured static routing tables depending on which interfaces are active. For a dismounted soldier, this means that a static routing table directs packets addressed to the squad toward the squad radio and packets addressed to the platoon toward the platoon radio. Communication with other groups or users must also be pre-configured to one of the radios as the outgoing interface.

For users connected to a vehicle LAN, another routing table is used instead. Internal vehicle traffic and traffic appropriate to send via the vehicle radio are routed toward the LAN. Normally this means that traffic to the platoon is transmitted on the LAN and traffic toward the squad is sent on the squad radios. The switch between the different routing tables occurs automatically whenever a user connects to the vehicle LAN or disconnects from the LAN. In that way, the individual soldiers do not need to do anything beyond connecting and disconnecting to the LAN when entering and leaving the vehicle, i.e. no change of the settings on the SN or the radio.

Handling autonomous networks means that all IP addresses on the radio networks must be preconfigured or self-configured. Communication with the squads and platoons also use preconfigured multicast IP addresses that are unique for each squad or platoon.

To handle the mobility of the SN, in terms of where it attaches to the IP network, IGMP (Internet Group Management Protocol) [6] can be used for multicast traffic. IGMP is a communications protocol used in IP networks to establish multicast group memberships. Most traffic in this environment is group communications. As long as the groups are preconfigured, The SN can transmit on each interface IGMP messages containing the information about the groups that are transmitted over that interface. That is, IGMP messages can be sent on the squad radio and platoon radio when the user is dismounted; otherwise it is sent on the vehicle LAN.

Voice group management based on SIP is assumed to require support from the vehicle router. On the vehicle LAN, the router dynamically assigns IP addresses to the assigned nodes, which may be the same every time a user mounts the vehicle.

All use cases can be handled by using this type of solution, but require that a number of parameters are preplanned. Examples are IP addresses on the radio interfaces, the SN multicast group membership, and which interfaces the information should be routed to, where the routing tables are functions of the active interfaces. Use Case 4 allows change only to a limited number of groups though, unless IPv6 is used. More details on the dual host solution can be seen in Appendix.

4.1.1 Ra 1570 – Harris 7800S

Ra 1570 (Harris 7800S) is expected to be the primary platoon radio in the near term. The Ra1570 radio is a layer 3 device, i.e., it contains a router. As it is mostly capable of handling static routing and lacks support for protocols such as IGMP, it is unclear how well Use Cases 2 and 5 can be handled. To handle multicast traffic passing the vehicle router, special treatment of this radio is needed. We do not have a general solution, although there are some ways to handle this problem, assuming that the radio can be configured to retransmit IP multicast packets. This means that a multicast packet arriving on the fixed wire interface of the radio is delivered on the wire interface of all other radios.

One option is to make a static IGMP join for the relevant multicast groups on the vehicle router's Ra 1570 interface; this is normally used when hosts are not capable of generating IGMP messages. In this case it means that the vehicle router always transmits on the pre-allocated interface, independently of whether users are there or not. In addition, we will probably have to be careful when using PIM-SM (Protocol Independent Multicast-Sparse Mode) [8] for these multicast groups. If more than one router must be configured with a static IGMP join to the same Ra1570 network, the use of PIM-SM might generate duplicate multicast traffic. It is unclear how to solve this problem. Using static IGMP joins without PIM-SM may work for Use Case 2, but it does not allow hosts interested in other groups to receive data and requires more preconfiguration of the vehicle routers.

Furthermore, in Use Case 5, data from the extended company network would always be transmitted on the radio network and increase the traffic load even when not needed. Moreover, only one vehicle in each platoon network should be configured with a static IGMP join in Use Case 5. Otherwise, we get duplicate multicast transmissions.

4.1.2 Limitations of the dual host principle

Here we list some limitations of the dual host principle that are not obvious from the use cases.

Limited unicast support

It can be complicated to handle unicast traffic because the IP address changes whenever a user mounts or dismounts a vehicle. However, similar problems occur for all mobile hosts in IP networks. Different solutions have been developed for such networks, and some, e.g. SIP, may be used here.

As long as all unicast sessions are initiated by a SN to a fixed address, i.e. not to another mobile node and the SN does not change position in the network during the session, unicast should work.

The cases where we have problems though, if no extra support for mobility is added, are the following:

- Unicast initiated by a SN that moves and thus changes source IP address.
- Unicast initiated by another node (e.g. another SN) which does not know the current address of SN.

The first creates a problem when a user mounts or dismounts as this would require a re-initiation of the unicast session. It should be noted, though, that in most cases a SN communicates with another SN, and the complexity of this problem is dependent on the crypto solution.

If tunnel mode is used and the system uses red IP addresses, those addresses do not have to change—only the black side addresses have to change. One SN could thus include a mobility update to inform the other SN about the address change. This, however, would not resolve the second problem, i.e. how to find the address of the mobile SN to begin with.

Unicast data communication initiated by an external node that needs to reach the mobile SN is a more difficult problem, though.

No re-routing between the black interfaces

If we use the dual host solution, there is little possibility of rerouting packets between the two radio interfaces. Static routing could be used, but needs to be manually set up, i.e. the SN cannot automatically reroute packets from one radio interface to another. Except for some specific cases, it should probably be avoided as the risk of loops is large.

An alternative is to let the applications retransmit data from the red side. For example, a squad leader receiving position information from its squad may choose to retransmit this data to the platoon. From a routing point of view, the retransmitted information would be handled as a new packet.

Single interface multicast groups

A multicast group must be sent on a single interface. Preplanning such a group to be sent on more than one interface creates problems as the SN has to use different source IP addresses for the different interfaces. The network will then most likely retransmit all packets on all interfaces. This is a problem if the interfaces are connected via a router somewhere else in the network, in which case this router should transmit the data on both interfaces. Problems occur if the interfaces are connected only intermittently.

4.2 Commercial router

In this case, the SN contains a commercial router that can run dynamic routing protocols on all its interfaces. Both unicast and multicast routing can be handled. In essence this would make the SN function as any other router in an IP network (almost at least; physical limitations remain, such as the amount of traffic that can be handled and the number of interfaces it has).

An advantage of this type of solution is that in theory it should be able to handle all use cases and be very adaptive to unplanned changes. Using common routing protocols also ensures good compatibility with other commercial routers in the network, which, it is hoped, will enable efficient route choices. IP addresses do not change as the users switch attachment, which simplifies the handling of unicast traffic. Moreover, also with this solution, there are similar limitations as in the dual host solution, with Ra1570 used as a platoon radio, see section 4.1.1.

A full router solution entails certain risks:

- It may not be possible to procure within the current time frame of SN, due to SN restrictions on physical size and power consumption.
- It is not clear today whether the amount of administrative routing traffic can be sufficiently reduced to be feasible on a typical tactical mobile radio network.

We will not go into the same details for this solution as for the previous dual host solution as it follows civilian standards to a very large degree, whereas the dual host solution would have to be specifically designed for SN.

Although the use of a commercial router means that the SN would be capable of supporting a large number of protocols, some of these standard protocols would be of more interest than others in the use cases describing tactical environments. Versions of Open Shortest Path First (OSPF) [9] are the most likely candidate for a unicast routing protocol, and although the use cases we have shown mostly could be described as broadcast radio networks, the networks can be expected to change very quickly. It is therefore expected that OSPF with MANET extensions, see e.g. [10], may be required in many parts of the network just to handle the changing environment.

A potential problem with this type of algorithm is protocol overhead, however. The basic idea of OSPF is to flood all link changes in an area; in that way all nodes in the area can calculate the best path to all other nodes within that area. The more routers that are located within the area, the higher the overhead will be. Moreover, updates are mostly sent if there are actual link changes. The more changes that occur in the network, the more signalization will be the result.

Adding a router to all SNs can thus potentially create problems, as in most of the described use cases the number of routers increases significantly from one in all vehicles to the cases where all soldiers are a router. This also results in increased protocol overhead in all networks, which might be a problem in the narrowband radio networks.

Estimating when this becomes a problem is not trivial as most evaluations on OSPF with MANET extensions are done specifically for mobile ad hoc networks. Protocol overhead in these networks, especially when they grow in size, is significant. For example, in [11] the total protocol overhead is simulated for the different MANET extensions compared with normal OSPFv3. For 50 node networks, they show overhead that varied from a few 100kb/s to significantly more than 1 Mb/s, depending on settings, density, and mobility. Note that this only includes overhead traffic generated locally within the network; part of this traffic must also be flooded throughout the OSPF area. Smaller networks generate less overhead but may be affected by other networks within the OSPF area.

However, none of the relevant use cases include mobile ad hoc networks; broadcast networks change less and should therefore generate a lot less overhead. In addition, current tactical ad hoc networks tend to hide ad hoc functionality on lower layers, which prevents the worst spreading of signalization. It is therefore somewhat difficult to say whether a commercial router solution will have difficulties with protocol overhead.

It should also be noted that the behavior of the network with this type of solution might be somewhat unpredictable for the user.

4.3 Compatible router

In this case the router used in the SN would not be a commercial router, e.g. Cisco, but rather a router optimized for the limited capacity of tactical environments. It would still have to support most (or all) of the standardized protocols as an interface to the less mobile parts of the network would be required.

Potential advantages of this type of solution would be a significant reduction in protocol overhead in some tactical networks. Major drawbacks, however, are compatibility problems as different implementations need to interact. With sufficient product testing and evaluation, it may be possible, though.

Furthermore, it is not obvious that the complexity of this type of solution is much less than that of a commercial router, which means that battery time might still remain an issue.

In addition, as the vehicle router is a commercial router, it is difficult to see any advantage of this type of solution in the use cases described in Chapter 3. Communications to and from this router must follow standard protocols. It would be very difficult to design protocols that would reduce the overhead in any significant manner.

An advantage of this solution would be where man-pack radios communicate without vehicle router support; then routing from one radio interface to another radio interface is needed. However, it is not clear why such functionality would be the responsibility of the SN, as only a small fraction of the SNs would be used in such cases. It would be more efficient to add the functionality to the man-pack radio instead (or a full commercial router).

5 Concluding remarks

We have examined the routing functionality in the Soldier Node. To evaluate different routing principles we have defined five use cases based on the Swedish Armed Forces' requirements on the Soldier Node. The following routing principles are considered:

- *Host*—The Soldier Node behaves in a similar way as a regular laptop connected to a network with an Ethernet interface.
- *Dual host*—The Soldier Node behaves as two different hosts as seen from the IP network. To control how the traffic is routed, it internally switches between preconfigured static routing tables depending on which interfaces are active.
- *Router*—The Soldier Node contains a router that runs dynamic routing protocols on all its interfaces.

We have shown that some routing functionality is required, i.e. a *host* solution does not fulfill the requirements on Soldier Node. With sufficient preconfiguration, a *dual host* solution can handle all of the use cases described in the report, but have some limitations, e.g. with respect to unicast traffic and with Ra 1570 used as a platoon radio in some of the use cases.

A *router* solution in Soldier Node has some attractive benefits: (1) routing is efficient, (2) the application IP address is independent of mobility, and (3) compatibility with other commercial routers in the network. It is unclear, however, whether such a solution can be implemented in the short term due to restrictions on power consumption and physical size. Moreover, also with this solution, there are similar limitations as in the dual host solution, with Ra1570 used as a platoon radio.

It is also unclear how well commercial router implementations behave in the narrowband tactical communication systems due to their potentially high overhead. A non-commercial router in Soldier Node, which is designed for low overhead in tactical environments, does not reduce the total overhead in a system that already has commercial routers.

6 References

[1] “Request for Information - Soldier Node”, FMV Document ID 367742, 2012-05-09

[2] A. Olsson, “Utkast Taktisk Teknisk Ekonomisk Målsättning (UTTEM) för Buret Krypto”, (fastställt), Försvarsmakten, HKV beteckning 12839:81884

[3] Harris RF-7800S, http://rf.harris.com/capabilities/tactical-radios-networking/rf-7800s

[4] Harris RF-5800H-MP, http://rf.harris.com/capabilities/tactical-radios-networking/rf-5800h-mp.asp

[5] Selex PRR, http://www.selexelsag.com/internet/localization/IPC/media/docs/MM07077_PRR_LQ.pdf

[6] B. Cain, “Internet Group Management Protocol, Version 3”, RFC 3376, October 2002

[7] J. Rosenberg et al., “SIP: Session Initiation Protocol”, RFC 3261, June 2002

[8] B. Fenner et al, “Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)”, RFC 4601, August 2006

[9] J. Moy, “OSPF Version 2”, RFC 2328, April 1998

[10] R. Coltu et al, “OSPF for IPv6”, RFC 5340, July 2008

[11] A. Roy Ed. and M. Chandra, Ed., “Extensions to OSPF to Support Mobile Ad Hoc Networking”, RFC 5820, March 2010

[12] T. Henderson, P. Spagnolo, and G. Pei, *Evaluation of OSPF MANET extensions*, Boeing Technical Report: D950-10897-1, July 2005.

7 Appendix—Details around dual host solution

We show some examples of technical solutions based on the dual host principle. For simplicity, the IP addresses are chosen to be simple to read not to be actual suggestions.

7.1 Use Case 1

The first use case describes soldiers communicating within their own squad; communication must be possible both as a mounted and as a dismounted user, see Figure 2. Each SN has static IP addresses on the squad and platoon radio interface according to Table 1; note that SN 1.5 has no radio in this use case. On the LAN, the router dynamically assigns IP addresses to the assigned nodes (may possibly be the same every time).

Table 1 IP address in Use Case 1. Addresses within parenthesis are not used at the moment in this use case.

Soldier Node	Squad interface address	Platoon interface address	LAN interface address
1.1	(1.1.1.1)	(1.2.1.1)	3.1.1.1
1.2	1.1.1.2	1.2.1.2	-
1.3	(1.1.1.3)	-	3.1.1.3
1.4	1.1.1.4	-	-
1.5	-	-	3.1.1.5

The squad has a static multicast address of 224.1.1.1. Both squad radio and platoon radio interfaces shut down if the user connects to the LAN.

SN units automatically send IGMP reports for joins of group 224.1.1.1 to the router on its squad radio interface if it is active; otherwise it sends it on its LAN interface. Inside the SN, multicast group 224.1.1.1 is statically directed toward the squad radio interface if not connected to the LAN; otherwise, it is directed to the LAN interface. The IP address 224.1.1.1 may be used by any user in the vehicle to reach the full squad no matter where they are.

There is no way to separate a soldier outside the vehicle from a soldier inside the vehicle that is connected to the vehicle LAN. If a user enters another squad's vehicle, it is not able to communicate with the other squad without further reconfiguration of the SN, i.e. the other squad's multicast address will be required in such cases. See case 4 to handle the former of these problems.

7.2 Use Case 2

This use case describes platoon communication and includes multiple vehicles, see Figure 3. Each SN has IP addresses according to Table 2. The IP addresses of squad 1 follows the same addressing principle as in Use Case 1.

Table 2 IP addresses in Use Case 2. Addresses within parenthesis are not used at the moment in this use case.

Soldier Node	**Squad interface address**	**Platoon interface address**	**LAN interface address**
1.1	(1.1.1.1)	(1.2.1.1)	3.1.1.1
1.2	1.1.1.2	1.2.1.2	-
2.1	1.1.2.1	1.2.2.1	-
2.2	1.1.2.2	1.2.2.2	-
3.1	1.1.3.1	1.2.3.1	-
3.2	1.1.3.2	1.2.3.2	-
3.3	(1.1.3.3)	-	3.1.3.3

SN 1.1 is also connected to the LAN (with 3.1.1.1 as before) as is SN 3.3, with 3.1.3.1. The platoon radio interface of SN 1.1 is disabled when it is connected to the LAN. The platoon has a static multicast address of 224.1.2.1. SN1.1 and SN3.3 automatically send IGMP reports on their LAN to join groups 224.1.2.1 when attaching to their LAN.

7.3 Use Case 3

In this case, the network is autonomous and cannot use the vehicle IP routers for assistance, see Figure 4. On the other hand, little or no communication with the outside world would also be assumed. In general, we have the same assumptions as in the previous two examples. This case motivates the use of fixed IP addresses for the squad radio network and platoon radio networks. Routing tables are static all through this use case. SN, 1.1 sends traffic to group 224.1.1.1 on its squad radio interface and traffic to group 224.1.2.1 on its platoon radio interface. SN 3.3 sends traffic to group 224.1.1.3 on its squad radio interface and traffic to group 224.1.2.1 on its platoon radio interface.

7.4 Use Case 4

In this use case some soldiers change their squad memberships, see Figure 5. We need a systematic IP-address assignment, so that IP-addresses are unique independent of which nodes that switch membership. The membership change for SN 2.1 now alters the IP address of the squad radio interface to 1.1.1.11. In addition, the IP address for SN 3.2 is changed to 1.1.1.22.

Depending on the number of IP addresses available for preconfiguration, this can be done without involving the vehicle router. The required number of IP addresses depends on the total number of groups that must be available to a user. If a connection to the vehicle LAN is required, the IGMP information must be updated as well. It is only possible to change to groups that are pre-configured. With IPv4, the numbers of available groups is limited. With IPv6, the number of available IP addresses is much larger, and a more efficient auto-configuration of IP addresses is possible. This allows a much larger number of available groups.

7.5 Use Case 5

In this case, the company network is extended to dismounted units, see Figure 6. We assume that SN X and SN Y are platoon leaders. Y is dismounted. Z is the company leader and is also dismounted. We also assume that 224.5.1.1 is the multicast address of the extended company network. A dismounted SN sends IGMP reports to join group 224.5.1.1 on the platoon radio interface. Once it is connected to the LAN, it transmits this IGMP report on the LAN instead, preventing traffic to this group from being transmitted on the platoon radio network. X, Y, Z are all handled similarly.