Fraunhofer FKIE

FRAUNHOFER INSTITUTE FOR COMMUNICATION, INFORMATION PROCESSING AND ERGONOMICS FKIE

CoNSIS

REQUIREMENTS REGARDING IP-BASED RADIO DEVICES IN HETEROGENEOUS NETWORKS

REQUIREMENTS REGARDING IP-BASED RADIO DEVICES IN HETEROGENEOUS NETWORKS

Christoph Barz, Harald Bongartz

Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE
in Wachtberg, Germany.

Project number: 100 021

Hartmut Seifert

IABG mbH
in Ottobrunn, Germany

Content

1 Introduction

During the CoNSIS experiments conducted in June 2012 in Greding, different radio devices were integrated into a common overlay network. Not all of these radio devices used interoperable waveforms and thus the interoperable systems formed closed network segments, which were connected via Internet Protocol- (IP-) based routers.
In this document, we describe the requirements for IP-enabled radio devices which were identified in the CoNSIS field experiments. In particular, these include requirements that arise from the nature of heterogeneous wireless networks with different technologies as well as from the use in the context of a coalition deployment.
Radio devices in the CoNSIS scenario act as wireless bridges. The various radio devices are connected to a router with CoNSIS extensions for heterogeneous wireless networks.
Not included in this document are requirements for IP-routing components in wireless devices that also act as routers. These were documented in CoNSIS separately as standard network profiles. In addition, at the present time no reliable statements about the required data rates at the application level can be made, since they are very specific and depend both on the used C2IS and on the particular application scenario. In particular for SOA-based C2IS, a broadband waveform (see COALWNW) should be available. The reduced range compared to many narrowband systems can largely be compensated at least in a convoy scenario via multi-hop transmissions. Using multi-topology routing even narrow-band radio systems with low data rates can be incorporated, but these will not be available for all data. In addition, the administrative overhead of routing increases with additional topologies in multi-topology routing, thus reducing the available data rates for user data.
The model employed in CoNSIS, in which the radio devices act as wireless bridges, is also endorsed by others. A study of the MIT Lincoln Laboratory funded by the United States Air Force comes to similar conclusions although this study was not designed to look into coalition operation explicitly. Their conclusions were published in an IETF draft (B. Cheng, L. Veytser, D. Ward, Radio to Router Interface Framework and Requirements, draft-bcheng-r2ri-framework-00, February 2012). A summary of these results can be found in the appendix (see section 3).
From these parallels can be deduced that the requirements are reasonable for both the national level and for coalition operations.

2
Radio Device Interface

From a router perspective, the number of local interfaces types should be kept as small as possible. At the same time it should be possible to exchange performance-based information with a radio.
As a flexible, universal and robust interface, a twisted-pair Ethernet-based interface (different speeds, typically 100 Mbit/s) has proven successful in the CoNSIS field tests. However, this type of interface hides radio specific behavior of a device from the network interface of the router.

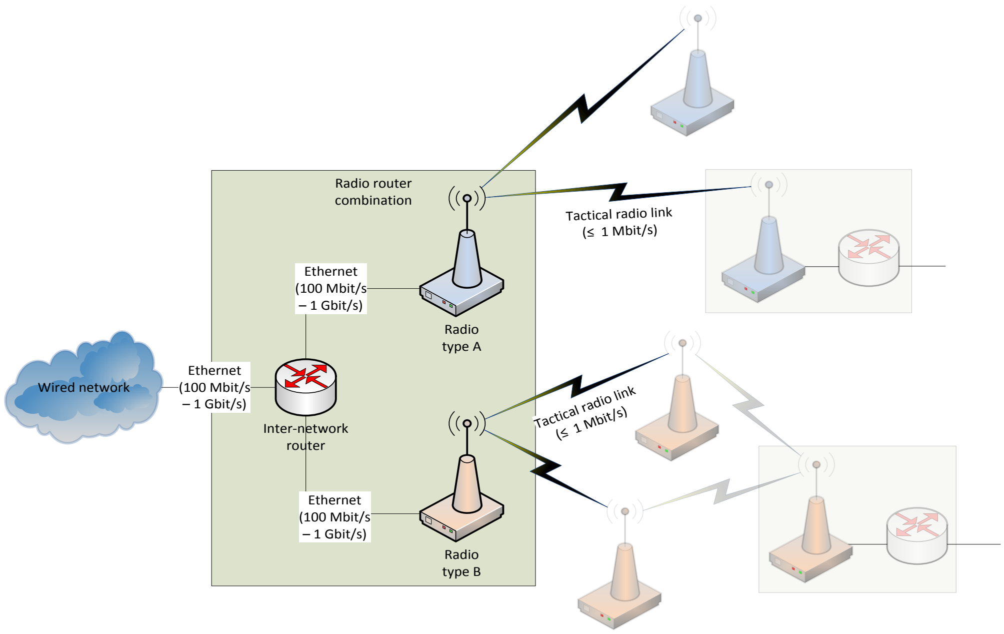

Figure 01: Combinations of router and different radio devices in a tactical network

Recommendations:

- Twisted Pair-based Ethernet has proven successful as interface to the radio devices, with 100 Mbit/s (IEEE 802.3u) or 1 Gbit/s (IEEE 802.3ab).
- The Ethernet interface should be used for user traffic as well as for the control of the radio device via the router.

Alternative interfaces were not examined systematically in the CoNSIS project.

2.1 Buffers within the radio devices

The radios that use Ethernet interfaces generally operate with a much lower transmission rate on the radio side. It is therefore necessary to be able to perform a rate adaptation of the data flow. There are two modes of operation:

- The radio buffers the IP PDUs (Protocol Data Units) provided by the router in an internal memory usually of unspecified size. It transmits the PDUs via the radio interface as soon as resources become available. This behavior is acceptable if there is no steady stream of data from the router, but rather a burst-type transmission behavior and the radio link is not overloaded. Ideally, this behavior is transparent to the router.

- The radio device sends status information about the radio channel and the amount of data in the internal buffers to the router, allowing a reduction of the router's sending rate (flow control).

In general, both methods can be combined. Even with the use of flow control mechanisms data has to be buffered to a small extent.
Some of the radios used in CoNSIS come with very large buffers. Radios with these characteristics typically buffer traffic over a longer period (up to several minutes in the CoNSIS field tests). All IP PDUs, regardless of their origin and nature, are cached in the buffer without further differentiation, with the result that time-critical information, e.g. update packages of the external routing protocol, will be transmitted by the radio device with a huge delay. As a result, changes in the network topology will not be considered in a timely manner by the corresponding routers.
The primary buffer control should preferably be a router functionality. Only when the data is buffered in the router instead of the radio device, it is ensured that QoS-based queuing mechanisms of the router will work correctly. A prerequisite for this is to limit the data transmitted to the radio devices. This can preferably be done dynamically via a flow control mechanisms, but also statically by shaping the traffic to the radio on the router side.

Recommendations:

- Radio devices should support flow control mechanisms (see also Quality of Service support).
- Radio devices in bridge modus should only have small buffers on the transmission path.
- For radio devices that form a mesh/ad hoc network, buffer sizes and queuing mechanisms should be flexibly configurable.

Further research is needed regarding flow control mechanisms in ad hoc radio networks.

2.2
Quality of Service support

For the realization of a consistent quality of service concept, the combination of quality of service mechanisms in a tactical router, at OSI layer 3, and in the radio devices, namely at layer 2, is important. This is especially true for radio equipment in the tactical area, since the available data rates are relatively low. A preferred treatment of certain data from other participants of the radio network can for example be enforced via a prioritized access to the wireless medium, via a time division approach for different traffic types, or via a dynamic reservation of communication resources. This is particularly important for VoIP based voice transmission.
In the experiments, a mismatch of DSCP values (Differentiated Services Code Point) interpretation in the radio devices with the CoNSIS DSCP semantics used by the routers was observed. In this case, the CoNSIS IP packages were downgraded, which affected multi-topology routing. This shows that all the QoS mechanisms have to be well aligned and that radio devices with multi-hop capability require larger integration efforts.

Recommendations:

- Radio devices should support layer 2 QoS mechanisms that complement the layer 3 mechanisms of the tactical router.
- QoS mechanisms of radio devices should be configurable in a flexible way.

2.3
Native support of voice transmissions

Language can be transferred via VoIP as normal IP traffic. This will require special QoS mechanisms (see section 2.2). For tactical use, it is also reasonable that the radio device provides a native digital voice transmission (e.g. as a push-to-talk), which is still functional within transmission range when the IP-based network has collapsed. When such mechanisms are used, it is crucial that these are integrable into a SIP-based exchange system for VoIP.

Recommendations:

- If the radios support a native voice transmission, this should be done digitally and seamlessly fit into the IP data transport.
- The native voice transmission mechanisms of the radios should be integrated in a SIP-based VoIP service.

A solution for integrating native voice transmissions with a SIP-based VoIP service is currently being developed within the project QUAKSBw.

2.4
Routing

2.4.1
Topology control and routing metrics

The transmission rate of the radio is usually not constant. Instead, it varies due to external influences, either due to the receiver signal strength variations (e.g. during the movement of nodes) or due to external interference. As a result, the transmission speed a radio device can offer to a router is not constant but varies with time.
To abstract from short-term fluctuations in the transmission rate, in CoNSIS different transmission classes were defined (with a variably adjustable upper and lower limit), where signaling the transmission speed is only needed when a threshold in either direction is exceeded. For the router, it is only important to know which transmission class is available at what time for a specific interface in order to perform its routing decisions.
There are different ways a router can determine the transmission speed (and other QoS - related parameters):

- a PPPoE-based approach which is common but is better suited for point to point connections (tunnel based approach without real multicast support), or
- a DLEP-based approach which has been developed for mesh networks which as yet has no finalized standard.

Especially for older radio device models, the changes in physical parameters are often not reported.
PPPoE and DLEP also offer support for flow control, so that the QoS queuing mechanisms of the router can work properly and an excessive buffering of data in the

radio can be avoided. Please note that an appropriate PPPoE of DLEP protocol instance is needed also on the router side.
If neither PPPoE nor DLEP is supported, only statically configured transfer classes and rate limitation on the router interface can be used to reduce the negative effects.
Routing in wireless networks should consider the quality of each radio link in the routing decision. For this purpose, the radio device has to provide the raw data regarding the state of each radio link depending on the routing metric used.

Recommendations:

- Radio devices should allow control and monitoring by a connected router.
- Control parameters should include: maximum data rate of the radio; actual data rate to each communication partner; reachability of the remote radio; usage of queues; additional relevant QoS parameters according to the layer 2 data model of QUAKSBw.
- All parameters required for the link metrics used in routing should be provided by the radio.
- To be able to work as a transparent layer 2 bridge, the radio should know the IPv4, IPv6 and MAC address of the remote routers and inform the local router via the local radio-to-router interface. This eliminates or reduces ARP or Neighbor Discovery requests via the radio interface.
- PPPoE Extensions (RFC 5578) or Dynamic Link Exchange Protocol (DLEP) should be used. DLEP is currently in the standardization process but does support multicast and does not require tunneling of data. General requirements for radio-to-router communication interfaces are provided by B. Cheng, L. Veytser, D. Ward, *Radio to Router Interface Framework and Requirements*, draft-bcheng-r2ri-framework-00, February 2012.

Additional research is needed with respect to a dynamic consideration of the condition of the individual radio links in multi-topology routing, and with respect to a refinement of cross-layer mechanisms.

2.4.2
Radio device – internal routing

Some wireless devices with Ethernet interface act as transparent bridges with or without multi-hop capability. Other radio devices provide IP routing functionality. To integrate the latter type of radio devices in a technology or vendor heterogeneous system, however, the radio devices must be integrated into the overall routing concept of the tactical network. This imposes special requirements regarding the support of special routing protocols (e.g. multi-topology routing). However, as mentioned in the introduction, these are not explicitly part of this document. If these routing protocols are not or not properly supported (incompatibility at the protocol level), the routing functionality of the radios must be turned off.
To integrate them as bridges in an ad hoc enabled, heterogeneous wireless network, the multi-hop capability of wireless devices imposes a special challenge. It is not clear to the tactical routers how many radio devices are actually on a path to another tactical router.

Recommendations:

- To integrate a radio device into a heterogeneous network, the internal routing of the radio as well as the multi hop capability should be deactivatable.

- As an alternative, information regarding the topology of the radio devices has to be accessible by the tactical router. This is of special importance for multi-hop capable radio devices that act as bridges. However, to the best knowledge of the authors, no solution is currently available.

2.4.3
Radio device – external routing

Due to problems regarding the integration in heterogeneous ad hoc networks, radio devices with their own routing capabilities were either not used in CoNSIS or their routing capabilities were suppressed. For this reason, no reliable statements regarding requirements for their use at domain boundaries (e. g. BGP support) can be made. Because of the reduced exchange of information between domains - a detailed view of the network is available only within a domain – mechanisms such as multi-topology routing can be implemented across domains only with restrictions. For this reason, the whole mobile CONSIS scenario was organized as a single routing domain.

Recommendations:

- Domain boundaries at radio devices should be avoided. However, these can only occur with wireless devices with router functionality.

2.5
Multicast support

Radio is in general a broadcast medium. The ability to explicitly address all stations in its range should be supported by the radio device. This is interesting both for applications that require efficient point-to-multipoint communication, as well as a requirement for the operation of most routing protocols. A more sophisticated group management is possibly supported by the router through additional multicast routing protocols.
Some radio device types offer the opportunity to define groups at layer 2. However, this form of explicit group management at lower layers is not recommended because configuration and integration are problematic.
Therefore it is not recommended to locate an explicit group management in the radios.

Recommendations:

- Radio devices should support the efficient transport of multicast data (RFC 1112, Level 2)
- Radio devices in bridge mode must support the transmission of IP broadcast and multicast packets to all 1-hop neighbors. Additional multi-hop relaying is only performed at tactical router level.
- Radio devices do not need to support multicast groups. Radio devices with multi-hop capabilities need to support a suitable multicast forwarding protocol which is optimized for radio networks, e.g. Simplified Multicast Forwarding (SMF), RFC 6621. In this case, these multicast mechanisms must be interconnected with multicast solutions for traditional IP networks (e.g. PIM-SM).

2.6
Additional management interfaces

In addition to the radio to router interface for radio link quality information, a radio device should include additional management interfaces that are accessible via IPv4 and IPv6 and cover all functionalities of the device. For radio devices with multi-hop capabilities, access to the topology of the radio network is very important.

Recommendations:

- For each functionality of the radio device, a corresponding management interface should be available.
- The management interface should support access via IPv4 and IPv6 based via SNMPv3 (RFC 3410-3418, STD0062) or – if there are no safety requirements - SNMPv2 (RFC 1901/1905/1906).
- An appropriate management information base (MIB) shall be provided and maintained.

3 Appendix

As part of the IETF Draft (B. Cheng, L. Veytser, D. Ward, *Radio to Router Interface Framework and Requirements*, draft-bcheng-r2ri-framework-00, February 2012), which is based on the results of a study of the MIT Lincoln Laboratory sponsored by the United States Air Force, the following assumptions with respect to a radio-to-router communication protocol were made:

1) **Radio Bridge-Mode Capability**
   Many current military and some commercial radio systems have built-in routers that perform layer-2 (intra-subnet) or layer-3 multi-hop routing. While there are techniques that can be used to bypass these built-in routers, we assume that in the future, functionality will be built into radio systems to allow bypassing of built-in multi-hop routing techniques and allow the radio to act as a layer 2 one RF hop bridge.
   The radios used in CONSIS do not yet support this functionality. The overlay techniques used in the field experiments were able to suppress the built-in multi-hop routing mechanism of the radio devices. This, however, resulted in significant additional complexity and overhead.
   For this reason, it is necessary that the radio devices provide a corresponding bridge mode.
2) **Radio Broadcast and Multicast 1 Hop Support**
   We assume that given IP broadcast and IP multicast packets, the radio has the ability to pass the data to its 1-hop neighbors and does NOT do additional relaying without passing the packet to the multi-hop router.
3) **Radio Provisions to Obtain Required Link Metrics**
   Although any proposed R2RI will define required link metrics for radio systems to provide, it will NOT define provisions for acquiring or measuring the RF link for required metrics. It is assumed that radio systems will measure or acquire the information directly or indirectly through radio-specific signaling.
4) **Radio Provisions to Exchange IPv4, IPv6 and MAC-level Identifiers**
   To be able to allow the radio to act as a transparent layer-2 bridge, the remote router MAC addresses and IPv4/IPv6 addresses need to be known. Although R2RI might require this information to initialize per neighbor R2RI link metric sharing between the radio and router, we assume that the radio obtains this information through its own signaling.
   From the perspective of CoNSIS, such a mechanism would be desirable to prevent ARP or Neighbor Discovery requests via the radio.
5) **Radio Transmit Buffer Size**
   Managing flow control and QoS at multiple layers of the network stack is an extremely complicated process. Ideally, QoS should be managed at the layer which handles multi-hop transmissions and short queues implemented in lower layers. R2RI protocols can therefore assume that flow control is managed top-down and not additionally re-managed at lower layers.
6) **Router Logically Separate from Radio**
   The primary benefit of R2RI is the ability to make routing decisions regarding different radio links, including links from disparate heterogeneous radio technologies.
7) **Radio-to-Router Connection Bandwidth vs. Over-the-Air Bandwidth**
   It is assumed that the available bandwidth between the radio and router physical connection is significantly higher than the over-the-air bandwidth available for data transmission. This ensures no bottleneck in control traffic transmission between the radio and router.

Thus, the MIT team with focus on national operations and the CoNSIS team with focus on coalition operations come to very similar conclusions. This suggests that the assumptions and requirements are generally useful for military radios.