Resource Management in Tactical Military Networks

Martin Lies[1], **Peter Sevenich**[1], **Christoph Karg**[2], **Christoph Barz**[3]
[1]FGAN-FKIE, Neuenahrer Straße 20, 53343 Wachtberg, Germany
[2]FH Aalen, Beethovenstraße 1, 73431 Aalen, Germany
[3]University Bonn, Römerstraße 164, 53117 Bonn, Germany

email: {lies|sevenich}@fgan.de / christoph.karg@fh-aalen.de / barz@cs.uni-bonn.de

Abstract

We present the concept of a network resource manager for tactical military computer networks based on the Internet Protocol Version 6. This manager is a security gateway with a number of enhanced functionalities. In particular, the gateway supports priority based services and efficient bandwidth management. Furthermore, it is capable to handle secure multicast communication.

1 Introduction

From a topological point of view military computer networks are comparable to their civil counterparts, because both consist of various LANs which are connected via an Internet. This suggests the assumption that civil networking technology is usable in military networks without problems. In case of strategic networks this is surely true, because the deployed hardware/software and the work flow are similar.

Things change if we consider tactical networks. The two main reasons are as follows. Firstly, the networking hardware is very heterogeneous and ranges from wirebased Fast Ethernet to ISDN and wireless from 802.11 to HF. Each type of link has different properties with respect to bandwidth, delay and error rate. Secondly, many of the required network services are of pure military kind and are not or only partially covered by COTS products. Some typical requirements are:

- *Multicasting:* The hierarchical organization of military units involves information propagation from only a few sources to many destinations. Using multicast for such kind of applications optimize the amount of data to be transmitted. Although there exist civil applications for multicast, this type of IP communication is not supported by major ISPs. Reasons may be that broadband networks can handle large amount of data and that the ISPs billing system is volume-based.
- *Restricted transmission modes:* Emission Control (EmCon) and Minimize Mode are transmission modes where the military units have to keep radio silence or to restrict the quality of the messages, respectively. In “classical” communication these modes can be enabled easily by command. In terms of computer networks this task is more complicated, because of the talkativeness of the IP protocol. Concretely, there is a lot of background communication in IPv6 such as routing or DNS requests which cannot be turned off without causing trouble.
- *Priority driven transmissions:* Military communication classifies a message according to the priority of transport. This categorization is applicable to computer-based message handling in a similar fashion.

Lies, M.; Sevenich, P.; Karg, C.; Barz, C. (2006) Resource Management in Tactical Military Networks. In *Military Communications* (pp. 7-1 – 7-12). Meeting Proceedings RTO-MP-IST-054, Paper 7. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
DEC 2006	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Resource Management in Tactical Military Networks	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **FGAN-FKIE, Neuenahrer Straße 20, 53343 Wachtberg, Germany**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM202750. RTO-MP-IST-054, Military Communications (Les communications militaires), The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**26**	

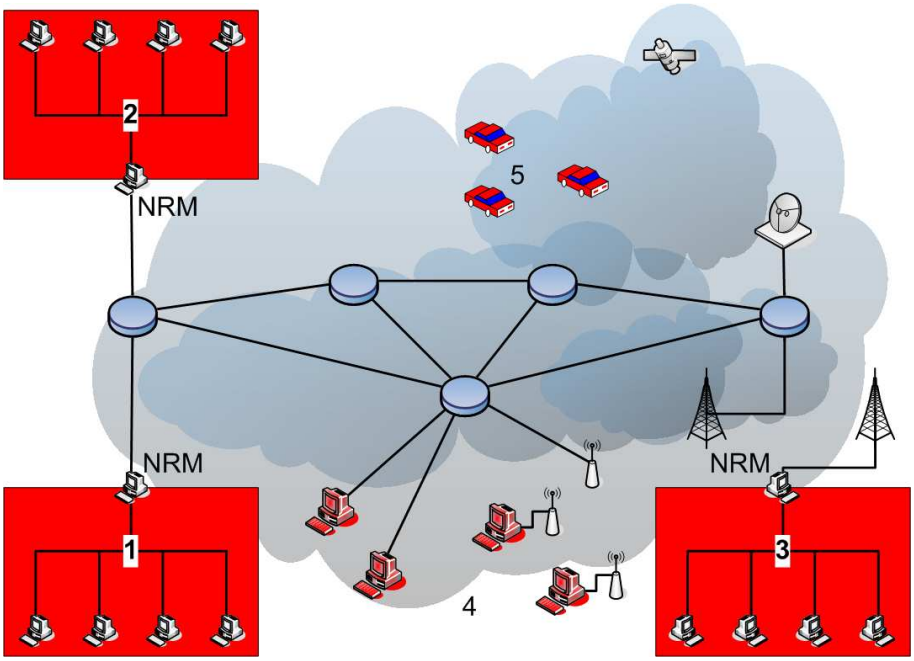


Figure 1: Different settings

To put the concept into practice, the network infrastructure must support priority-based transport of datagrams.

Besides the points mentioned above, secure communication is a mandatory requirement. Usually, tactical networks are set up as VPNs. As a consequence, the network splits up in secure (red) and insecure (black) subnets. An important role falls to the security gateway which is responsible for the control and protection of the incoming and outgoing traffic of one red subnet.

The network resource manager (NRM) has to be able to support a number of different scenarios as can be seen in figure 1. The most common scenario is the communication between two red subnets (1 and 2), each guarding the data at a central point. Other possibilities are shown with groups 3-5. A complete subnet (group 3) could be connected through a tactical link (i.e. HF). Single systems could be used in a more mobile environment with the use of MANETs (group 4) or even satellite (group 5). Each of these scenarios has its own set of requirements and challenges.

2 Architecture and Overview

The architecture of the Network Resource Manager is as shown in figure 2. All modules communicate across a central component, the *Network Resource Core* (NRC). The main task of the NRC is to ensure that every packet to be transmitted across the black connection is modified according to the policies and informations supplied by the activated modules before being encrypted by IPSec.

The routing together with the overlay-control modules are described in section 3, information about QoS and priority management can be found in section 4, security-related matters are in section 5 followed by a discussion about bandwidth management in section 6.

One important part of the NRM is the *Bandwidth Information Protocol* (BIP). This XML-based protocol is the interface on both sides of each NRM, to the applications inside the local red subnet and to the other

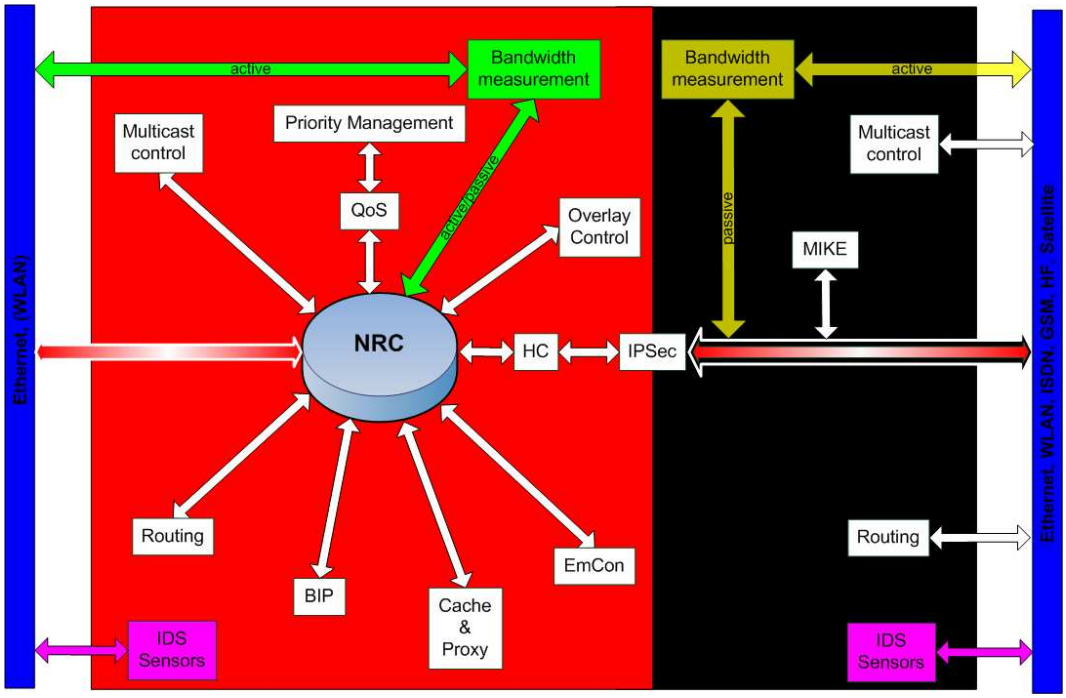


Figure 2: The NRM architecture

NRMs across the IPSec-secured connections. A first step in developing this protocol is to collect all the types of informations to be distributed across the participants.

The various applications are able to either request (*pull*), automatically receive (*push*) or subscribe to a hybrid mode, which pushes warnings after reaching a specified threshold. The informations are extracted from the bandwidth management module, the overlay control and all the other sources inside the NRM. For example, a VoIP-application could receive regular reports about the available bandwidth for a certain priority, adapt the codec accordingly and even inform the user of an imminent connection loss.

In between the NRMs the BIP is used to distribute informations about routing alternatives according to the overlay control module and exchange bandwidth, delay and jitter information from the bandwidth management module.

On both sides of the NRM are the interfaces which are to be supported. While there are no real limitations on the black side of the NRM, obviously only secure media should be considered on the red side.

3 Routing

Since the NRM is an enhancement of a security gateway the support of IPv6 routing is one of its central functionalities. Standard unicast routing via the OSPF or the RIPNG protocol is to be supported as well as stateless/stateful auto-configuration. Additionally, the NRM acts as a multicast router. In this case, we differ between two scenarios. If the black network supports multicast, then the NRM can use it directly. As a consequence, information about group structure leaks from the red into the black subnet. On the other hand, if the black network has no multicast capability, then the NRM has the responsibility to perform an additional address translation and distribute the multicast packets. Necessary for this kind of multicast support is an efficient key-management (MIKE) for IPSec that supplies the different group-operations inherent to a multicast-enabled environment as introduced in [1, 2].

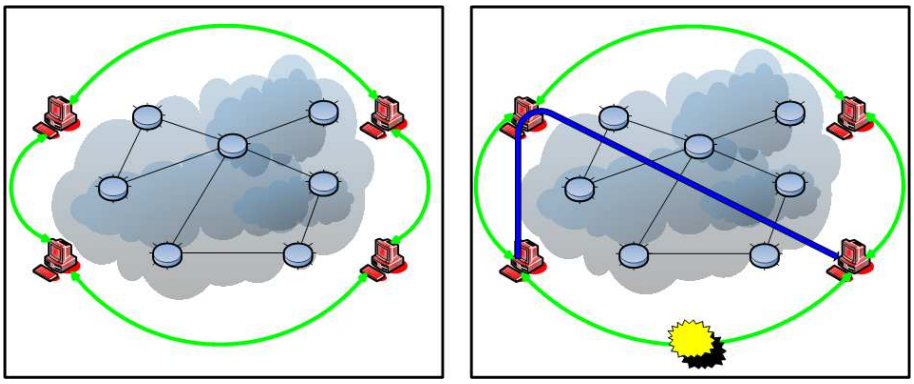


Figure 3: Overlay functionality

Another property is the support of resilient overlay networks. On an abstract level, the Internet is able to automatically detect defective connections and find alternate routes between two partners. The problem of course is that these mechanisms need time to distribute the new informations and adapt the relevant routing entries.

The concept of resilient overlay networks (RON) [3] describes the idea that cooperating systems can detect and also react faster to outages by rerouting the data across other known connections [4].

To be able to support this, the NRMs perform regular measurements between each other and exchange the necessary informations about alternative routes with corresponding bandwidth, delay and jitter. For this exchange, it is possible to use a link-state routing protocol or alternatively the previously proposed BIP because of its capabilities to transfer other relevant data between the NRMs. As soon as a connection is interrupted, the NRMs can then transport the data across a known alternative route (figure 3).

One of the remaining questions is the practicability of RONs across tactical data links and which modifications are necessary to ensure the full capabilities, especially in combination with IPSec, multicast and the other mechanisms necessary for bandwidth-reduction.

4 Priority Based Services

One of the principal duties is the management of military priorities in communication. A widely followed approach is the use of Differentiated Services (DiffServ) [5], where data is transported according to previously negotiated service level agreements. These agreements specify the available bandwidth and guarantee parameters like jitter and delay.

In a military context, this approach can not always be followed. The black Internet is usually not under military control, so with every provider there has to be a separate service level agreement negotiation, together with the corresponding charges. Also, DiffServ is not supported in every part of the Internet, so that even high priority data is transported as *best effort* together with everything else.

The modules *QoS* and *Priority Management* enable the NRM to actively support and, if necessary, adapt informations regarding the priority of data-packets or data-streams. For example, the VoIP-software *PCPhone* sets the Flowlabel and specific bits in the TrafficClass-field of the IPv6 header to mark the real-time packets and make them distinguishable from normal data. The NRM is able to detect these markings and transfer the packets with an according priority to their destination. At the same time, the NRM has to be able to reserve a narrow channel for system information like DNS queries or IPSec key management messages.

Another part of the priority based services is the ability to cache the most widely used services. Examples would be the Router Advertisement/ Neighbor Discovery messages, DNS or even http. All these requests are to be mirrored locally together with the corresponding answer from whichever system is responsible inside the secure subnets. Then, for a certain time-frame, following requests for the same information could be answered locally. After the specified time, the NRM is able to refresh the local entries autonomously, or lacking a certain number of requests, discards the cached information.

This mechanism can also be used to support EmCon (Emission Control), where the participant is placed under a one-sided radio silence. This raises a number of difficulties for the network protocols, starting with the IPv6 inherent mechanisms of router advertisement and neighbor discovery, routing updates over the TCP acknowledgement and retransmit mechanisms up the various application methods used. The EmCon-side would have to answer as many of the request locally as possible before discarding the rest, while the sender-side could implement further mechanisms to ensure a complete transmission of important data, similar to the TCP *fast-retransmit*-method.

Another problem is the end of the EmCon-mode. At his point, every system would try to update its information as fast as possible, generating a huge network-load and possibly even crashing parts of the communications system. The *restart* period has to be controlled very carefully.

5 Security Mechanisms

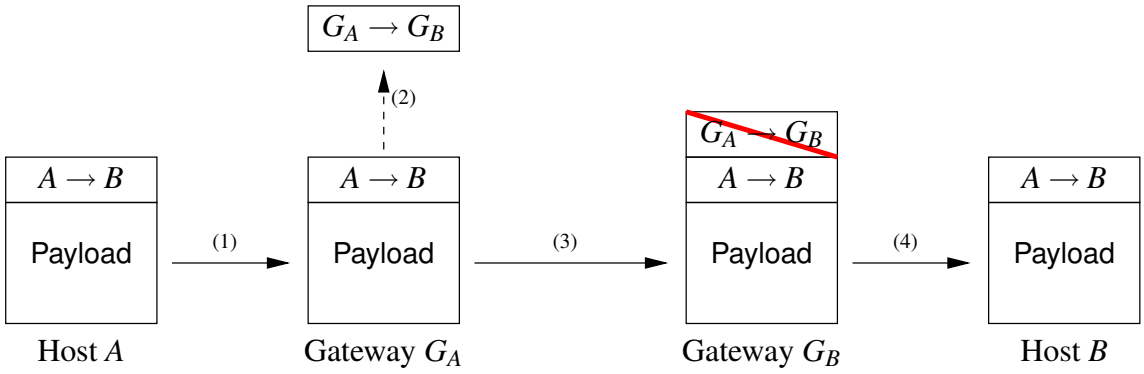
The Network Resource Manager integrates a number of security-relevant mechanisms in its architecture. The most important are described in the following sections.

IPSec The security of the data traffic is a mandatory requirement for military networks. In terms of computer networks this requirement is usually fulfilled by using the IP Security (IPSec) framework. Hence, the NRM is deployed with this functionality. More precisely, the network is divided in red subnets which are connected via a black Internet. While the the traffic within the red parts is regarded as safe, the black part is not safe. Therefore, all traffic passing through the black part must be secured. The NRMs take over this part by acting as security gateways. Each NRM is responsible for exactly one red subnet. It is connected to the other subnets via several secure IPSec tunnels. Together, all NRMs build up a complete mesh whose number of tunnels is quadratic in the number of NRMs.

Header Reduction The here described concept of the header reduction is based on the work described in [6]. As can be seen in figure 2, the header-compression is dependent on IPSec.

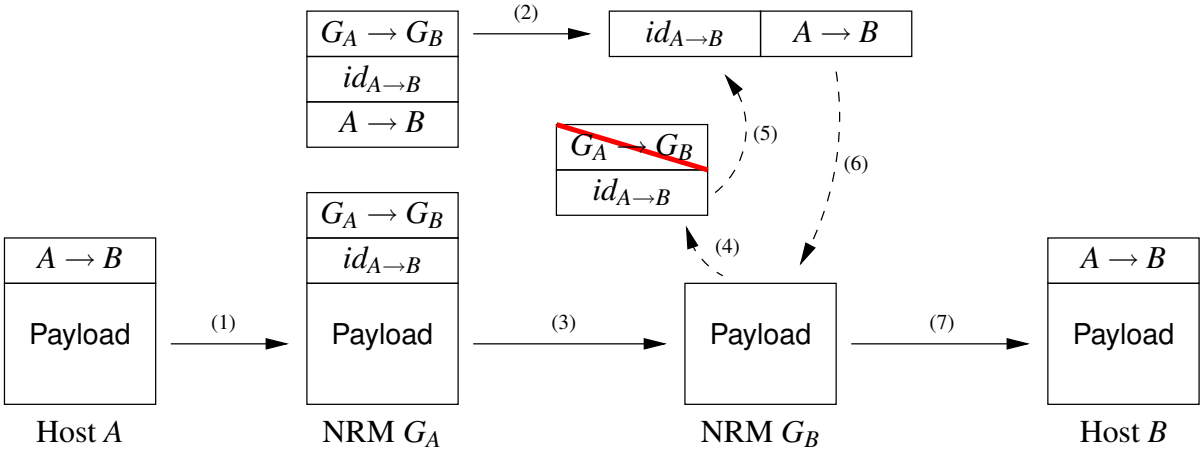
The tunneling of IP packets via IPSec provides security at the expense of larger IP packet sizes. The reason is that each IP packet, which has to be transmitted from one NRM to another, is embedded in another IP packet (for details see figure 4). Regarding IPv6, the size of each tunneled packet increases by at least 16 bytes. While this overhead is neglectable for broadband networks, it causes a noticeable reduction of data throughput in narrow bandwidth links.

In order to reduce the overhead of the transmitted tunnel packets, an alternative tunneling mechanism is proposed. From a technological point of view, the receiving NRM must get a piece of information on how to forward the content of an incoming tunneled packet. In terms of IPSec, this information is contained in the original IP header which is part of the tunneled packet's content. The idea is to replace the original IP header by a unique identifier. The procedure is illustrated in figure 5.



a) *IP Tunneling:* (1) Host A sends an IP packet to host B via the gateways G_A and G_B, whereat the link between G_A and G_B is an IP tunnel. (2) On receipt, G_A stores the IP packet in a new one. This mechanism offers several opportunities to manipulate the IP packet to be tunneled. For example, IPSec encrypts the packet before transmission. (3) G_A sends the resulting packet to G_B. (4) G_B unfolds the incoming packet, this is, it removes the tunnel header and forwards the content to host B.

Figure 4: Tunnel mode and header reduction.



b) *Header reduction:* Again, host A sends an IP packet to host B via the gateways G_A and G_B. (2) Instead of tunneling the packet directly, gateway G_B performs the following manipulation. Based on the IP header $A \rightarrow B$, G_A computes an unique identifier $id_{A\rightarrow B}$. (2) G_A sends the pair $(A \rightarrow B, id_{A\rightarrow B})$ to gateway G_B, which stores the information in an internal lookup table. (3) G_A replaces the header $A \rightarrow B$ by the corresponding identifier $id_{A\rightarrow B}$ and sends the result to G_B. This replacement is done for all following IP packets with header $A \rightarrow B$. (4) On receipt, G_B removes the tunnel header and the identifier. (5) G_B uses $id_{A\rightarrow B}$ to retrieve the the original header $A \rightarrow B$. (6) G_B combines $A \rightarrow B$ with the payload. (7) G_B forwards the original IP packet to host B.

Figure 5: Tunnel mode and header reduction.

Host Security Another part of security is host-based. This is resolved on one side through a careful configured stateful packet filter (i.e. iptables) and on the other side through an integrated intrusion-detection-system (IDS) (i.e. snort). This IDS could later on be enhanced to support domain-like structures as described in [7] and [8]. The advantage is that information about an occurring security-related incident, like worm or even hacker activities, against one NRM could be distributed to the other subnets. There the local administrators would be made aware of these activities and could initiate the appropriate countermeasures, for example securing the targeted services.

6 Efficient Bandwidth Measurement

Tactical military networks usually contain low bandwidth links. In order to use this limited resource more efficiently a header compression mechanism described in section 5 is integrated into the NRM. In addition to this static approach to reduce the bandwidth needed for communication, a dynamic bandwidth management concept is included in the NRM architecture. This concept is used to support dynamic applications that can adapt to the network resources offered by the management system. The requirement for bandwidth management is based upon the usage of low bandwidth links and real-time voice data streams. In case of multiple bulk data transmissions, bandwidth might be reasonably shared in a round-robin manner [9]. But a real-time voice data stream has specific bandwidth and delay requirements that must be met for a successful transmission. Otherwise, the stream can be canceled. The bandwidth management is introduced to allocate bandwidth for individual streams and to enforce priority based data transmission (cf. section 4).

In order to integrate the concept of dynamic bandwidth management into the NRM, different aspects of the design have to be considered. In this section measuring points and measurands are identified that provide information for the administration of available resources. In addition as stated in section 2 this information has to be distributed between the NRMs.

6.1 Resource administration and data distribution

Similar to the concept of RONs the communication structure of different NRMs naturally form a secure overlay network. The underlying, insecure data communication network provides IPv6 connectivity to the overlay. However, the underlying technology is transparent to the NRMs. One task of the NRMs is to monitor and administrate the resources provided by the overlay network. In order to get characteristics of the underlying network paths, corresponding properties have to be acquired and a communication infrastructure has to be established to distribute these information.

If the acquired path characteristics are shared between all peering NRMs, e.g. by BIP or a link state routing protocol on top of the overlay network (cf. section 3), a directed graph of the overlay can be constructed at every NRM. This information can be used for traffic engineering purposes (e.g. efficient bandwidth usage) and rerouting in case of path failure. Creating and distributing these topology database is the basis for resource administration within the whole overlay network.

Beside the path characteristics of the overlay network between the NRMs, end-to-end paths are also of interest. An end-to-end network path between two devices comprises the links between the clients and their NRMs in the red cloud. Keeping this information local can lead to congestion in target or transit networks. But sharing this information would increase communication overhead and complexity. Depending on the network characteristics, a solution is to distribute these additional resource information on demand.

6.2 Measuring points and data acquisition

After taking a look at the data administration and distribution perspective, this section concentrates on the decision where to introduce measuring points and which data acquisition approaches are chosen within the NRM architecture in order to get information about the communication peers, e.g. capacity and latency (section 6.3). Within the scope of tactical military networks, information has to be collected via two types of equipment: trustworthy (red) and unknown (black). At first, the scenario of one red cloud comprising at least one NRM and a set of trusted nodes is regarded, before the case of two red clouds connected via a black cloud is considered.

Within a red cloud at least three different approaches to acquire information about the network properties are envisioned. Firstly, information can be gathered dynamically, e.g. information can be collected with SNMP tools, network sniffers, and statistics can be collected from RMON probes [10]. Furthermore, additional techniques can be used that are described below in the context of two red clouds connected via a black one. Secondly, if a homogeneous network is present, device driver information can be used to evaluate network properties. This can be viewed as partly dynamic. Thirdly, if the red cloud is a mainly static or pre-planned network, properties can be configured in advance. Although the internal structure of a red cloud is of interest for management purposes, this paper concentrates on the next case, as these techniques can also be used within a red cloud.

If two red clouds are connected via a black transit network, the usable data acquisition procedures are restricted. On the one hand, the transit network might be part of a different administrative domain, which is not willing to offer information about structure and properties of the network. On the other hand, offered information is untrusted and must not be used for security reasons. In this case end-to-end measurements between NRMs connecting the red clouds can be used in this scenario.

End-to-end measurements can be classified as sender based or receiver based methods. Sender based methods consider information which is available at the sending node. In this context ICMP is one protocol that allows for sender based techniques. The tool pathchar [11] and [12] use or at least suggest ICMP to infer path characteristics or node traversal costs. Measurements performed with the sender based method have some drawbacks. At first, the node or path segment under investigation should reply on ICMP messages instantaneously, because an intra-node delay is part of the measurement. Secondly, measurements are subject to forward and reverse path effects, i.e. it might be difficult to distinguish between characteristics adhering to one path. For example, this method is subject to cross traffic on the down- and upstream path. Receiver based methods (sometimes referred to as sender-receiver based methods) use the cooperation between two nodes. One node generates data to be evaluated at the receiving node. This method needs access to both nodes and if the receiving node should consider all received packets, privileged access is needed (packet sniffing). One additional method, which can also be seen as a sub-category of the receiver based method, is the receiver-only based method [13], [14]. This method only relies on information available at the receiving node. Measurements need a careful analysis as the characteristics from the sending node must be taken into account, e.g. the receiver can not per se differentiate between delays caused by sending node or the network.

Another classification of end-to-end measurements is the distinction between passive and active methods. Passive measurement techniques rely on data that is injected into the network from other nodes or applications. Therefore, it does not perturb or influence the ongoing communication. Active measurements inject probes into the network or send purposive traffic patterns. If this method is used, one must be aware of its influence on other traffic, e.g. if one tries to gather the spare capacity of a network path by flooding, it will swamp out other TCP streams.

These lead to different approaches for end-to-end or more precisely NRM-to-NRM measurements in the context of the NRM architecture in order to acquire information about an untrusted transit network:

- passive, receiver-based measurements via the IPsec tunnel between two NRMs,
- passive, receiver-based measurements of the IPsec tunnel between two NRMs,
- active, receiver-based measurements via the IPsec tunnel between two NRMs, and
- active, receiver-based measurements between two NRMs beside the IPsec tunnel.

These four envisioned alternatives clearly have their advantages and disadvantages with respect to accuracy, additional overhead and security aspects in the context of military networks. As the properties of these approaches should be investigated either in a real life implementation or in the scope of simulation with different measurement techniques, up to now all of them are considered in the NRM architecture.

6.3 Measurands

Bandwidth, delay, jitter and loss rate of a network path are the main measurands when characterizing network performance. Accordingly, different applications have different requirements in terms of these measurands. While bulk data transfer mainly benefits from high network bandwidth, multi-media applications are more sensitive to delay and jitter. While the previous section describes possible measurement points in the NRM architecture, this section gives a brief overview of techniques for measurands.

So far, the most interesting measurand for the NRM is capacity, which is also referred to as bandwidth. The term capacity is often divided into path capacity and spare path capacity. While path capacity describes the maximum available capacity on a network path, spare path capacity describes the unused or free part of the capacity on a network path within a certain time interval. In both cases packet dispersion techniques [15] can be used to determine this quantity. One of the first well known papers describing the packet dispersion effect is [16]. Here, the packet dispersion effect is used to determine the time to inject new packets into the network, which is also known as the self-clocking effect of TCP. The underlying idea is to send packets back-to-back, i.e. as fast as possible, and analyze the signature when packets leave the network. Up to now, several papers and tools are using packet dispersion techniques to describe performance measures of IP networks. As a basic path capacity estimation technique for the NRM, the packet pair technique is under investigation [17]. Additionally, new research techniques like CapProbe [18] are also considered as extension to the basic packet pair technique.

The interaction of packet pair techniques and traffic shaping is of particular interest. To the best knowledge of the authors, insights in this area are rare. In the NRM context this interaction is of particular interest, because available DiffServ classes should be monitored and used for real-time voice traffic. Packet pair techniques in combination with traffic shaping methods, which are used to realize a specific DiffServ per-hop behavior, may result in estimations not corresponding to path capacity. For example in [17] a specific scheduling mechanism is used that fragments and prioritizes real-time voice data stream. Measurements in this context reveal information about the behavior of the shaping method and – according to the measurement setup – bandwidth estimates rather represent available capacity than path capacity.

In addition to capacity as a leadoff measurand, the NRM architecture can be used to acquire complementary information. As latency and jitter are also important in the scope of real-time voice transmission, these measurands should also be considered. While round trip time measurements can easily be collected, the one way delay or latency may induce additional hardware requirements (e.g. GPS) in order to get sufficiently accurate results.

Furthermore, capacity and delay measurements can be supported by additional inference techniques that try to detect characteristics of the underlying technology [19]. In environments, where the measurands are ambiguous, details about the network technology may reveal additional information or explain inaccurate measurands, e.g. in wireless scenarios. This method can assist measurements either within a red cloud or between NRMs.

7 Conclusion

We have introduced a new concept for the Network Resource Manager for tactical military networks. In this work we combine a number of elementary features like security through IPSec, the support of QoS and military priorities, modules for a more robust and bandwidth- efficient use of tactical connections together with methods for bandwidth-measurement and distribution of the acquired informations.

The goal of dynamic bandwidth management in the scope of tactical military networks, especially in conjunction with the NRM architecture, is to support adaptive applications that need a certain level of knowledge of the underlying network capabilities. Therefore, the topology and the properties of the interconnections need to be discovered. This can be accomplished by measurements based on the packet dispersion technique. The next steps in the area of efficient bandwidth management are investigations into packet dispersion techniques with respect to different measurement points and the distribution of the information between NRMs.

References

[1] T. Aurisch, C. Karg, *A Daemon for Multicast Internet Key Exchange*. IEEE Local Computer Networks, pp.368-376, 2003.

[2] T. Aurisch, *Using Key Trees for Securing Military Multicast Communication*. IEEE MilCom, 2004.

[3] D. Andersen, *Resilient Overlay Networks*, Master Thesis, Massachusetts Institute of Technology, May 2001.

[4] N. Feamster, D. Andersen, H. Balakrishnan, F. Kaashoek, *Measuring the Effects of Internet Path Faults on Reactive Routing*. ACM SIGMETRICS 2003, San Diego, CA, June 2003.

[5] K. Nichols, S. Blake, F. Baker, D. Black, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*. RFC 2474, December 1998.

[6] P. Sevenich, G. Beling, *Multiplexing Time-Critical Data Over Heterogeneous Subnetworks of Low Bandwidth*. Regional Conference on Military Communication and Information Systems RCMCIS, Zegrze, Poland, 1999.

[7] D. A. Frincke, D. Tobin, J. C. McConnell, J. Marconi, D. Polla, *A Framewrok for Cooperative Intrusion Detection*. Proc. 21st NIST-NCSC National Information Systems Security Conference, 1998.

[8] M. Jahnke, J. Tölle, M. Lies, M. Bussmann, S. Henkel, *Components for Cooperative Intrusion Detection in Dynamic Coalition Environments*. NATO/RTO IST Symposium on Adaptive Defence in Unclassified Networks, Toulouse, France, 2004.

[9] Shreedhar, Varghese, *Efficient Fair Queuing Using Deficit Round-Robin*, IEEE/ACM Transaction on Networking, Vol. 4, No.3, June 1996

[10] Waldbusser, Cole, Kalbfleisch, Romascanu, *Introduction to the Remote Monitoring (RMON) Family of MIB Modules*, RFC 3577, August 2003

[11] Jacobsen, *Pathchar: A Tool to infer Characteristics of Internet Paths*, ftp://ftp.ee.lbl.gov/pathchar, April 1997

[12] Bellovin, *A Best-Case Network Performance Model*, February 1992

[13] K. Lai, M. Baker, *Measuring Bandwidth*, in Proceedings of IEEE INFOCOM, March 1999

[14] K. Lai, *Measuring the Bandwidth of Packet Switched Networks*, Ph.D. Thesis, Stanford University, October 2002

[15] Prasad, Dovrolis, Murray, Claffy, *Bandwidth Estimation: Metrics, Measurement Techniques, and Tools*, IEEE Network, Nov/Dec 2003

[16] Jacobsen, *Congestion Avoidance and Control*, ACM SIGCOMM, September 1988

[17] Lies et. al, *THE EFFECTIVE QOS MECHANISM FOR REAL TIME SERVICES IN IP MILITARY NETWORKS*, Regional Conference on Military Communication and Information Systems RCMCIS, Zegrze, Poland, 2004

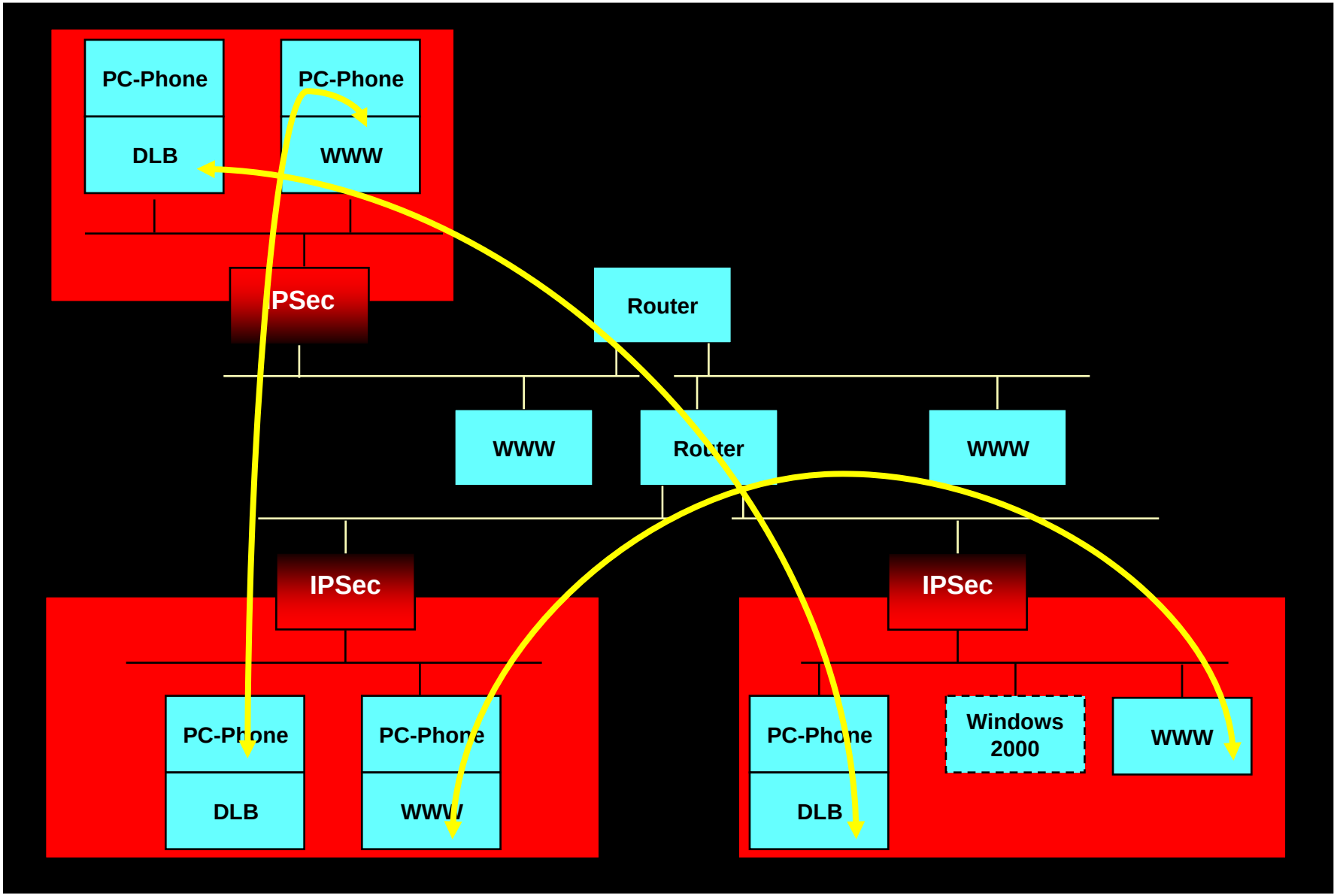
[18] Kapoor et al., *CapProbe: A Simple and Accurate Capacity Estimation Technique*. In Pro-ceedings of the ACM SIGCOMM, Portland, Oregon, USA, August 2004

[19] Marc Fouquet, *Detecting wireless Link Layers by using packet dispersion techniques*, Diploma Thesis, 2005

Resource Management in Tactical Military Networks

Martin Lies, Peter Sevenich, Christoph Karg, Christoph Barz

Secure Communication with IPSec in Tunnelmode

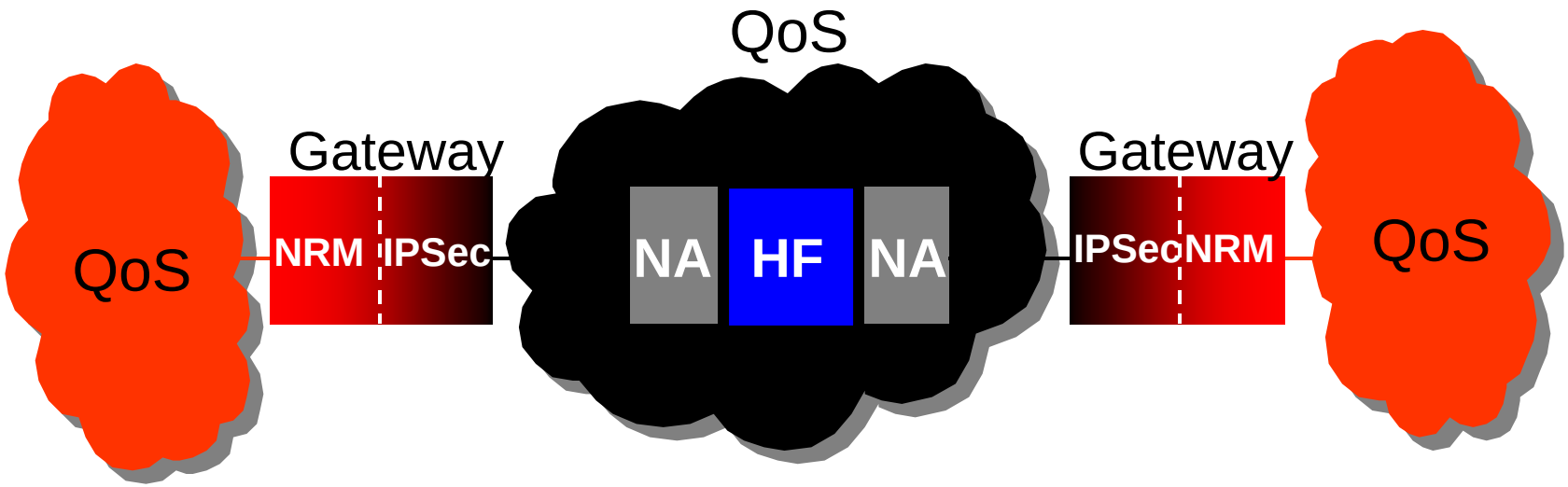


IPSec in Tactical Communications

- Strict separation of red and black network parts
- Atypical links in black network needed
  - e.g. narrowband links like HF/VHF are bottlenecks
  - other examples are mobile radio links or satellite links
  - impact on services (data, voice, multimedia, protocol information)
  - this calls for traffic control
- EMCON (simplex mode)
- Multicast Group communications

INSC Architecture and Network Resource Manager

•IPSec Gateway is a Bottleneck for Attacks and QoS

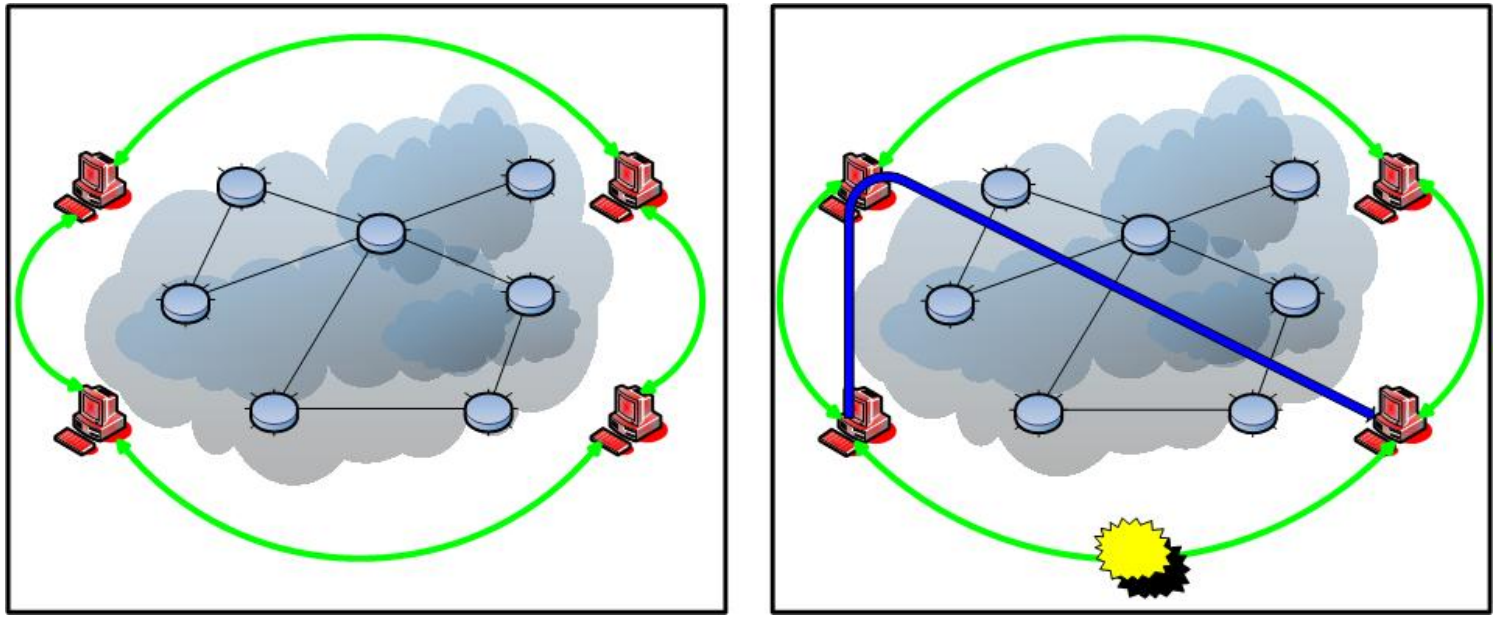


Goal: improved network performance and resource management

- Establish a tactical mode for the IPSec Gateway
- Put more Intelligence to the Gateway without modifying the IPSec
- Network Resource Manager uses GW-Information and Hardware

Routing in User Space (Overlay network)

NRM acts as router for Unicast and Multicast communication and exchanges routing information with NRM´s in other red subnets.

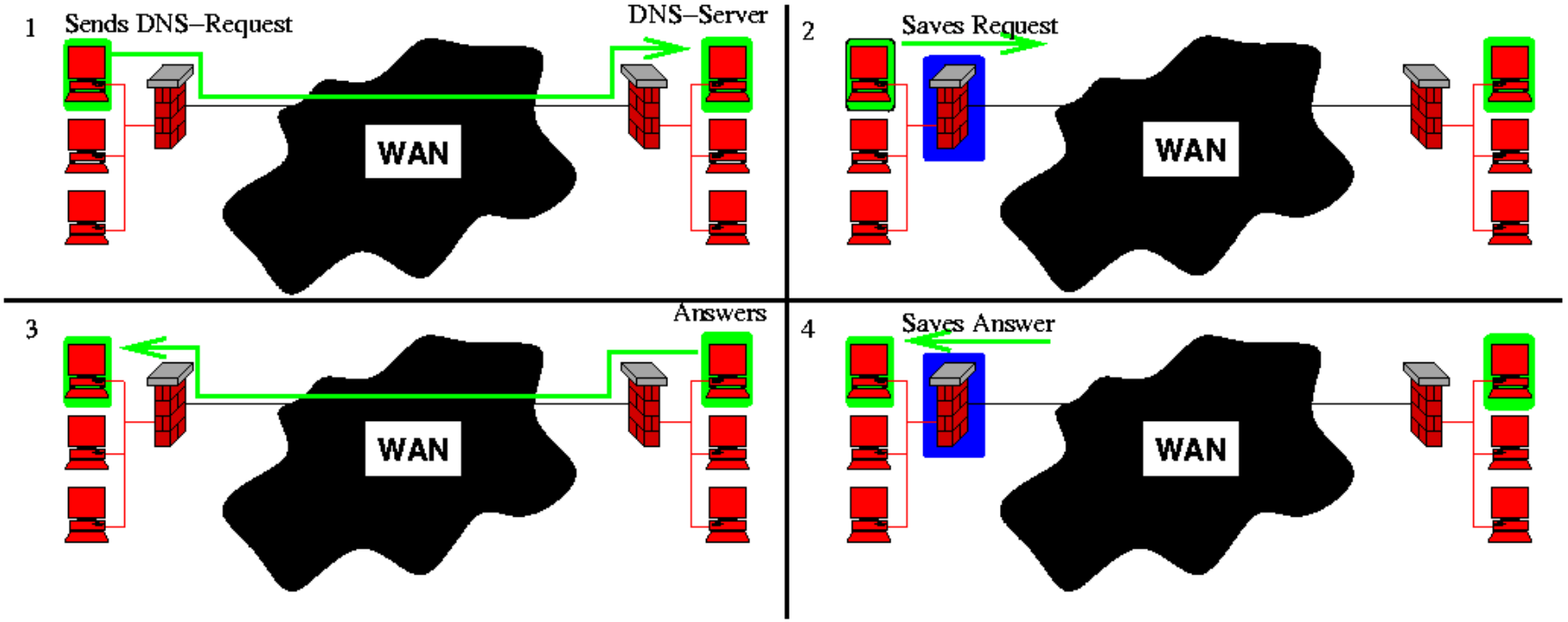


This guides to the idea of resilient overlay networks which can detect and react fast to outages by rerouting data across known connections.

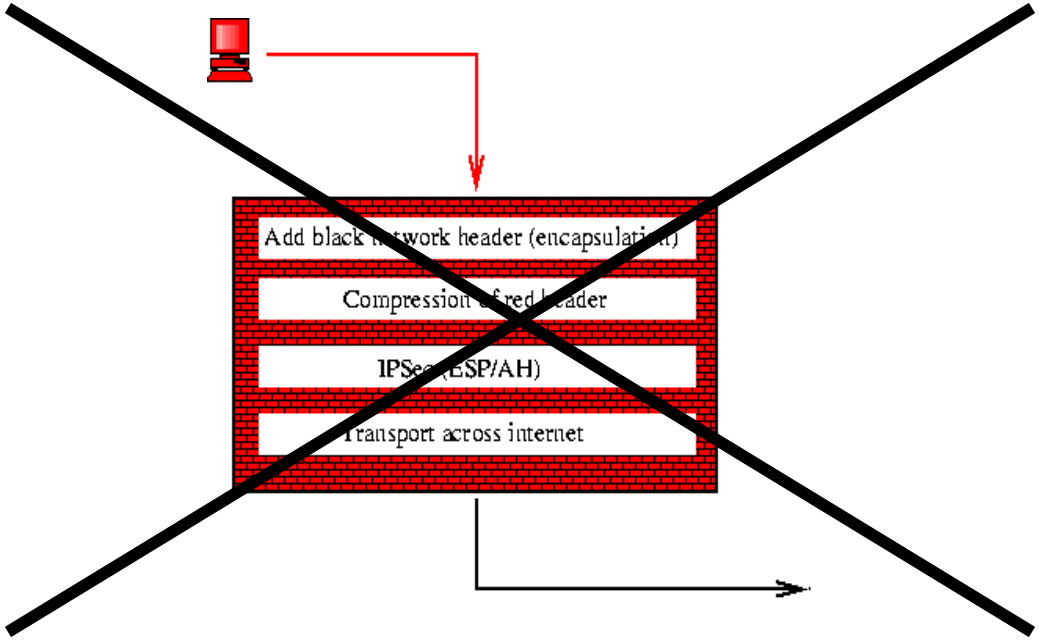
Caching of Service Information

Goal: reduce network load on narrow bandwidth links

Service examples: ICMPv6, NTP and OSPFv6



Red Header Compression in the NRM



After connection is established, index replaces the 40 Byte IPv6 header

- No red header compression in IPSec gateway
- Independence of kernel versions and updates (problem today)
- Reduces the header overhead (especially for VoIP)

QoS and Priority Scheduling

- QoS and military priorities
- NRM provides necessary intelligence in user space
- NRM needs bandwidth availability information > measurements
- Store per stream: priority, time-critical y/n, required BW, flow_id
- Scheduling algorithm uses this connection table
- In the black domain QoS by DiffServ and black Network Adapters > copy traffic class & flow label from red to black

Measurements and Hypothesis Testing

- Strict red-black separation > inability to directly exchange info (e.g. no ICMP message transfer & no red/black router comm.)
- Red network nodes implicitly make assumption on black links > risk of failure or sub-optimum QoS if atypical links (wireless)
- Better: set up & test hypotheses and measure parameters,
  - e.g. capacity of end-to-end path, available bandwidth
  - Hypotheses could be HF/VHF, SATCOM, mobile radio link
  - Measurements are also delay, jitter and packet loss
- There are publicly available tools e.g. to measure available BW
- Cooperation with University of Bonn, Computer Science IV

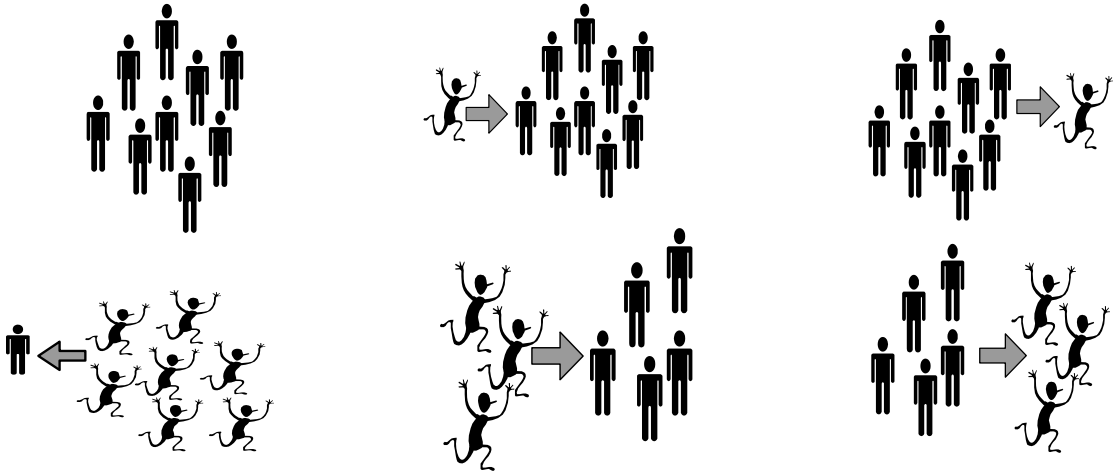
Bandwidth Information Protocol (BIP)

- BIP to exchanges information between NRM`s in the overlay network and applications inside red networks to communicate the available bandwidth
- Application can adjust e.g. by choosing proper voice coding rate

Multicast Key Management

- Internet Key Exchange (IKE) specifies protocol for automated negotiation of IPSec parameters
- If several subnets are connected via a narrow bandwidth link, load of negotiation for ***n*** subnets might be high

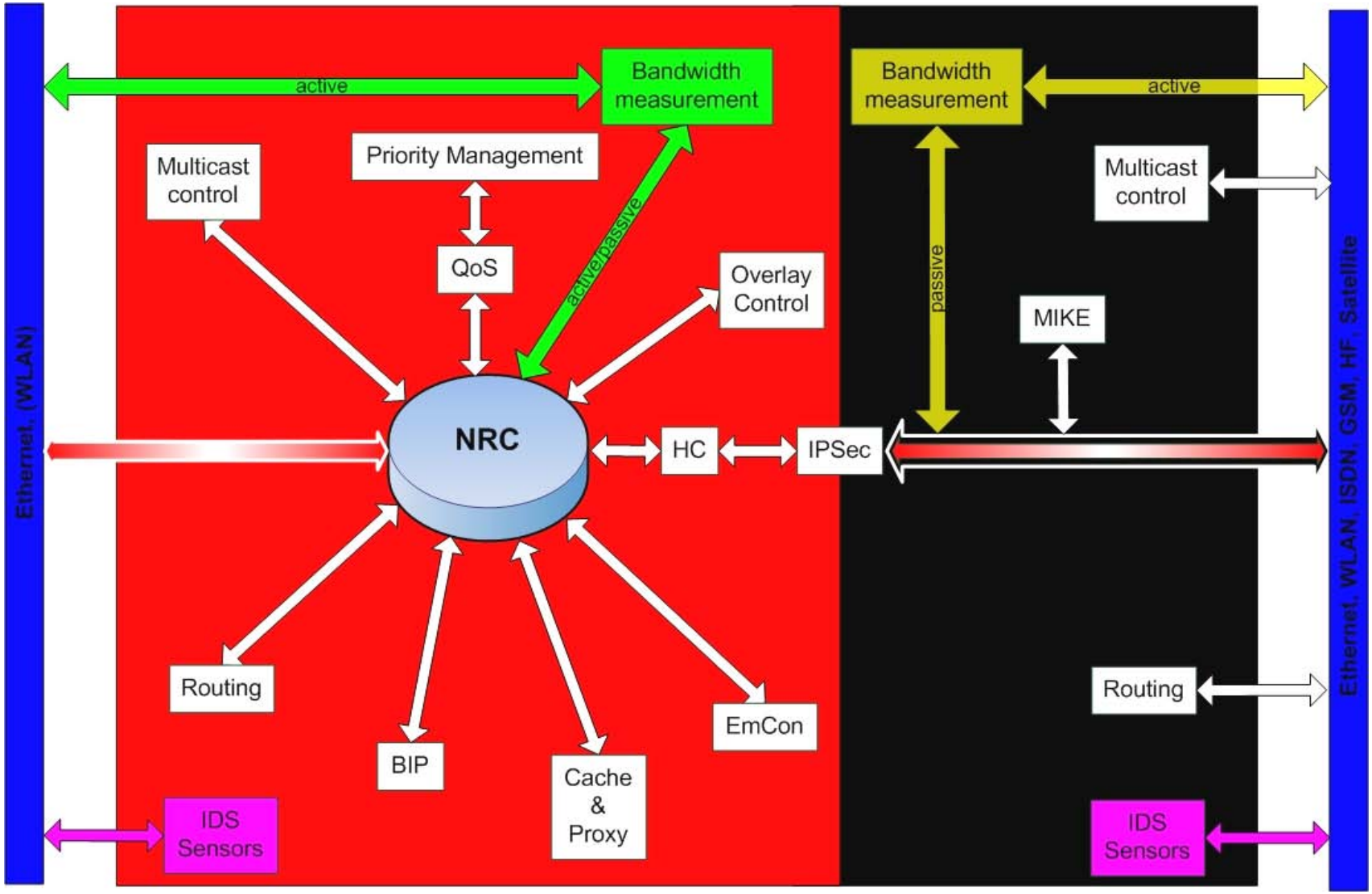
➢ The Multicast Internet Key Exchange protocol (MIKE) uses a group oriented approach for key exchange, IPSec gateways can easily join or leave the group



EmCon

- EmCon in IPv6 networks requires that no IP traffic is going out of the respective subnet or host !!
  This is a tough requirement – no routing, no management !!
- The NRM can simulate uninterrupted network connectivity by caching routing information
- The EmCon NRM can block outbound transmissions and accept only inbound traffic

NRM Architecture



Functionalities of the Network Resource Manager

- **Routing:** Unicast and multicast routing between red subnets
- **Caching of Service Information:** Reduction of network load (ICMPv6, NTP, OSPFv6, etc.)
- **Header Compression:** Use Improved Tunnel Mode
- **QoS & priority scheduling** by monitoring and handling multiple connections
- **Measurements and hypothesis testing** to support above scheduling
- **Bandwidth Information Protocol:** Signaling of available bandwidth to applications for application adaptation
- **Key Management:** Reduction of network load by IPSec gateway group key management
- **EmCon Functionality:** Use caching
- **Architecture:** Flexibility and independence from kernel versions by filtering with iptables + processing in user space + Headercompr.