EUR AMHS Documentation

IP Infrastructure Test Guidelines for EUR AMHS

EUR DOC 027 - Provisional Edition

IP Infrastructure Test Guidelines for EUR AMHS	
Document Reference:	EUR AMHS Documentation, IP Test Guidance
Author:	AFSG Planning Group
Revision Number:	Version 1.0
Date:	24/04/12
Filename:	IP Infrastructure Test Guidelines for EUR AMHS v1_0.doc

Document Control Log

Edition	Date	Comments	section/pages affected
0.1	03/05/2010	Creation of the document.	all
0.2	04/08/2010	Incorporation of review comments by DFS-CC, editorial improvements	all
0.3	24/08/2010	Incorporation of review comments, editorial improvements	all
0.4	17/02/2012	Change of the title, incorporation of comments	all
0.5	19/03/2012	Refinement of the document for presentation at AFSG/16	all
1.0	24/04/2012	Adopted version (AFSG/16)	

Table of contents

1 INTRODUCTION 6

1.1 PURPOSE OF THE DOCUMENT 6
1.2 OBJECTIVES OF THE IP INFRASTRUCTURE TESTS 6
1.3 DOCUMENT STRUCTURE 6
1.4 TEST OVERVIEW 7
1.5 SUMMARY OF THE IP INFRASTRUCTURE TESTS 7

2 IP INFRASTRUCTURE TEST – GENERIC ENVIRONMENT DESCRIPTION 8

2.1 GENERIC IP INFRASTRUCTURE DESCRIPTION (NETWORK ARCHITECTURE SCHEME) 8
2.2 GENERIC LOCAL IP INFRASTRUCTURE DESCRIPTION (LOCAL IP NETWORK SITE) 9
2.3 GENERIC WAN IP INFRASTRUCTURE DESCRIPTION 10
2.4 LEVELS OF INFLUENCE TO BE TESTED 11
2.5 IP TEST EQUIPMENT ("TEST DRIVERS") 15
2.5.1 Connection points of the test drivers 15
2.5.2 Short description of the tools mentioned above 16

3 IP INFRASTRUCTURE CONFIGURATION AND NETWORK PARAMETERS 17

3.1 DESCRIPTION OF THE IP INFRASTRUCTURE USED IN THE OPERATIONAL OR REFERENCE (TEST) ENVIRONMENT 17
3.2 LOCAL IP ADDRESSES 18
3.2.1 Local IPv4 addresses of Test partner A (known at own site, but not published) 18
3.2.2 Local IPv4 addresses of Test partner B (known at own site, but not published) 19
3.3 INTERNATIONAL IP ADDRESSES (LOCAL, LAN, WAN) 19
3.3.1 International IP addresses of Test partner A 19
3.3.2 International IP addresses of Test partner B 20
3.4 IP ROUTING REQUIREMENTS AND SETTINGS 20
3.4.1 WAN level 20
3.4.2 Local Level 20
3.4.3 End system setup 20
3.5 CONFIGURATION DETAILS, DEFINED FOR THE DIFFERENT LOGICAL CONNECTIONS IN THE DIFFERENT ELEMENTS OF THE INFRASTRUCTURE (ROUTERS, SWITCHES …) 21
3.5.1 Standard templates 21
3.5.2 Standard parameters and adjustments 21
3.5.3 Special parameters and adjustments for specific cases if required 21
3.5.4 Requirements to be fulfilled by the application host (parameters, settings …) 21

4 IP TEST PROCEDURES 22

4.1 IP REACHABILITY TESTS 22
4.1.1 IPT101 – Ping from Test Driver A to Test Driver B with 64 bytes 22
4.1.2 IPT102 – Ping from Test Driver A to Test Driver B with 1024 bytes 23
4.1.3 IPT103 – Ping from Test Driver A to Test Driver B with 2048 bytes 24
4.1.4 IPT104 – Ping from Test Driver B to Test Driver A with 64 byte 25
4.1.5 IPT105 – Ping from Test Driver B to Test Driver A with 1024 byte 26
4.1.6 IPT106 – Ping from Test Driver B to Test Driver A with 2048 byte 27
4.2 RECOVERY AFTER OUTAGE (IF NO REDUNDANCY AVAILABLE) 28
4.2.1 IPT201 – Outage of LAN connection to local router of Test Driver A 28
4.2.2 IPT202 – Outage of LAN connection to local router of Test Driver B 29
4.2.3 IPT211 – Outage of the local router of Test Driver A 30
4.2.4 IPT212 – Outage of the local router of Test Driver B 31
4.2.5 IPT221 – Outage of the connection between local router and firewall at site A 32
4.2.6 IPT222 – Outage of the connection between local router and firewall at site B 33
4.2.7 IPT231 – Outage of the firewall at site A 34
4.2.8 IPT232 – Outage of the firewall at site B 35
4.2.9 IPT241 – Outage of the connection between border router and firewall at site A 36
4.2.10 IPT242 – Outage of the connection between border router and firewall at site B 37

4.2.11 IPT251 – Outage of the border router at site A *38*
4.2.12 IPT252 – Outage of the border router at site B *39*
4.2.13 IPT261 – Outage of the connection between border router and WAN at site A *40*
4.2.14 IPT262 – Outage of the connection between border router and WAN at site B *41*
4.3 REDUNDANCY RECOVERY 42
4.3.1 IPT301 – Outage of LAN connection to one of the local routers of Test Driver A *42*
4.3.2 IPT302 – Outage of LAN connection to one of the local routers of Test Driver B *43*
4.3.3 IPT311 – Outage of one of the local routers of Test Driver A *44*
4.3.4 IPT312 – Outage of one of the local routers of Test Driver B *45*
4.3.5 IPT321 – Outage of the connection between a local router and firewall at site A *46*
4.3.6 IPT322 – Outage of the connection between a local router and firewall at site B *47*
4.3.7 IPT331 – Outage of the firewall at site A *48*
4.3.8 IPT332 – Outage of the firewall at site B *49*
4.3.9 IPT341 – Outage of the connection between border router and firewall at site A *50*
4.3.10 IPT342 – Outage of the connection between border router and firewall at site B *51*
4.3.11 IPT351 – Outage of the border router at site A *52*
4.3.12 IPT352 – Outage of the border router at site B *53*
4.3.13 IPT361 – Outage of the connection between border router and WAN at site A *54*
4.3.14 IPT362 – Outage of the connection between border router and WAN at site B *55*
4.4 PERFORMANCE TESTS 56

ATTACHMENT A: CHANGE CONTROL MECHANISM OF THE IP INFRASTRUCTURE TEST GUIDELINES 57

A.1 PROCEDURE FOR DEFECT REPORT (DR) 57
A.2 PROCEDURE FOR CHANGE PROPOSAL (CP) 57
A.3 TEMPLATE FOR DEFECT REPORTS / CHANGE PROPOSALS 58

References

[1] ICAO Annex 10 – Aeronautical Telecommunications, Volume II: Communication Procedures

[2] ICAO EUR Doc 020, EUR AMHS Manual, Appendix A

[3] ICAO EUR Doc 020, EUR AMHS Manual, Appendices D - F

[4] EUROCONTROL SPECIFICATION of Interoperability and Performance Requirements for the Flight Message Transfer Protocol (FMTP), Edition 2.0 - Released issue, 14/06/2007

Table of Figures

FIGURE 1: GENERIC IP INFRASTRUCTURE 8
FIGURE 2: DIAGRAM OF A GENERAL END TO END ARCHITECTURE USING PENS 9
FIGURE 3: GENERIC LOCAL IP INFRASTRUCTURE 10
FIGURE 4: GENERIC WAN IP INFRASTRUCTURE 11
FIGURE 5: LEVELS OF INFLUENCE IN A GENERIC NON-REDUNDANT IP INFRASTRUCTURE 12
FIGURE 6: LEVELS OF INFLUENCE IN A GENERIC REDUNDANT IP INFRASTRUCTURE 13
FIGURE 7: LEVELS OF INFLUENCE IN A GENERIC FULLY REDUNDANT (F. R.) IP INFRASTRUCTURE 14
FIGURE 8: CONNECTION OF THE TEST DRIVERS TO THE IP INFRASTRUCTURE 15
FIGURE 9: EXAMPLE OF A REDUNDANT IP CONNECTION (OPERATIONAL) 17
FIGURE 10: EXAMPLE OF A REDUNDANT IP CONNECTION (TEST) 18

List of Tables

TABLE 1: TEST SCENARIO OVERVIEW 7
TABLE 2: LOCAL IP ADDRESSES (TEST PARTNER A) 18
TABLE 3: LOCAL IP ADDRESSES (TEST PARTNER B) 19
TABLE 4: INTERNATIONAL IP ADDRESSES (TEST PARTNER A) 19
TABLE 5: INTERNATIONAL IP ADDRESSES (TEST PARTNER B) 20

1 Introduction

1.1 Purpose of the Document

1.1.1 The purpose of the document is to define a set of IP Infrastructure Tests from the viewpoint of the application in order to ensure the IP connectivity between application systems, e.g. AMHS, prepared for going into operation. The document defines the objectives and prerequisites as well as the set of IP tests themselves.

1.1.2 The IP Infrastructure Tests are connectivity tests and if available, tests of the IP redundancy. They should form a final part of the overall IP Infrastructure Acceptance Tests performed by ANSP's network teams.

1.1.3 Successful completion of these tests is a prerequisite for application tests (e.g. AMHS Interoperability Tests, AMHS Pre-operational Tests, or in case of the OLDI application: FDE/FMTP Interoperability Tests).

1.2 Objectives of the IP Infrastructure Tests

1.2.1 The objectives of the IP Infrastructure Tests are:

1. To test the IP connectivity between future application systems, e.g. AMHS, in a test and/or operational environment;
2. To test the recovery of non-redundant connections; or
3. To test the recovery of redundant connections; and
4. To measure the time the recovery takes.

1.2.2 The prerequisites of the IP Infrastructure Tests are:

- Successful completion of the WAN tests (in case of PENS: PENS Basic and Extended Tests);
- Successful test of the setup and IP routing mechanism of the local equipment on both sites (cf. 2.2) (Local IP Network Infrastructure).

1.3 Document Structure

1.3.1 *Chapter 1* presents the purpose, objectives and test overview.

1.3.2 *Chapter 2* contains a generic description of the environment to be tested including the test equipment which should be used for the IP Infrastructure Testing.

1.3.3 *Chapter 3* describes the IP infrastructure configuration, the Network parameter set-up and the IP routing requirements and settings.

1.3.4 *Chapter 4* contains the scenario description of the IP Infrastructure Tests procedures.

1.3.5 Attachment A provides the Change Control Mechanism for this document.

1.4 Test Overview

1.4.1 Following IP Infrastructure Tests have to be performed:

- IP Reachability Tests
- Outage and recovery tests

1.4.2 The tests are described in test scenarios – IPTxxx, where xxx is the scenario number. The following table contains an overview of the test scenarios:

Test-case id	Test function
IPT1xx	IP Reachability Tests
IPT2xx	Recovery after Outage
IPT3xx	Redundancy Recovery

Table 1: Test Scenario overview

1.4.3 Performance Tests are raised in Section 4.4

1.5 Summary of the IP Infrastructure Tests

1.5.1 After successful completion of the IP Infrastructure Tests the respective **test report** should contain:

- a section describing the concrete IP infrastructure which was subject of the test, including all necessary information for later maintenance and troubleshooting (cf. Chapter 2);
- overview of the tests which are the result of tailoring of the generic tests in adaptation of the above described IP infrastructure;
- the name of the tester(s);
- the date when the tests were performed;
- the result of each test case;
- the values measured where appropriate;
- the overall test result: "Successful (without remarks)",

  "Successful with remarks".

Note.- If the test was not successful which means not ready for the usage of the application all results should also be documented.

2 IP Infrastructure Test – Generic Environment description

2.1 Generic IP infrastructure description (Network architecture scheme)

2.1.1 The IP infrastructure under test consists of three different network segments:

- Local IP Network of ANSP A (Site A) – National IP segment Site A
- Wide Area Network (WAN) provided by ANSPs or a Service Provider. In case of PENS – PENS IP Segment.
- Local IP Network of ANSP B (Site B) – National IP segment Site B

2.1.2 A generic block diagram is provided in Figure 1.

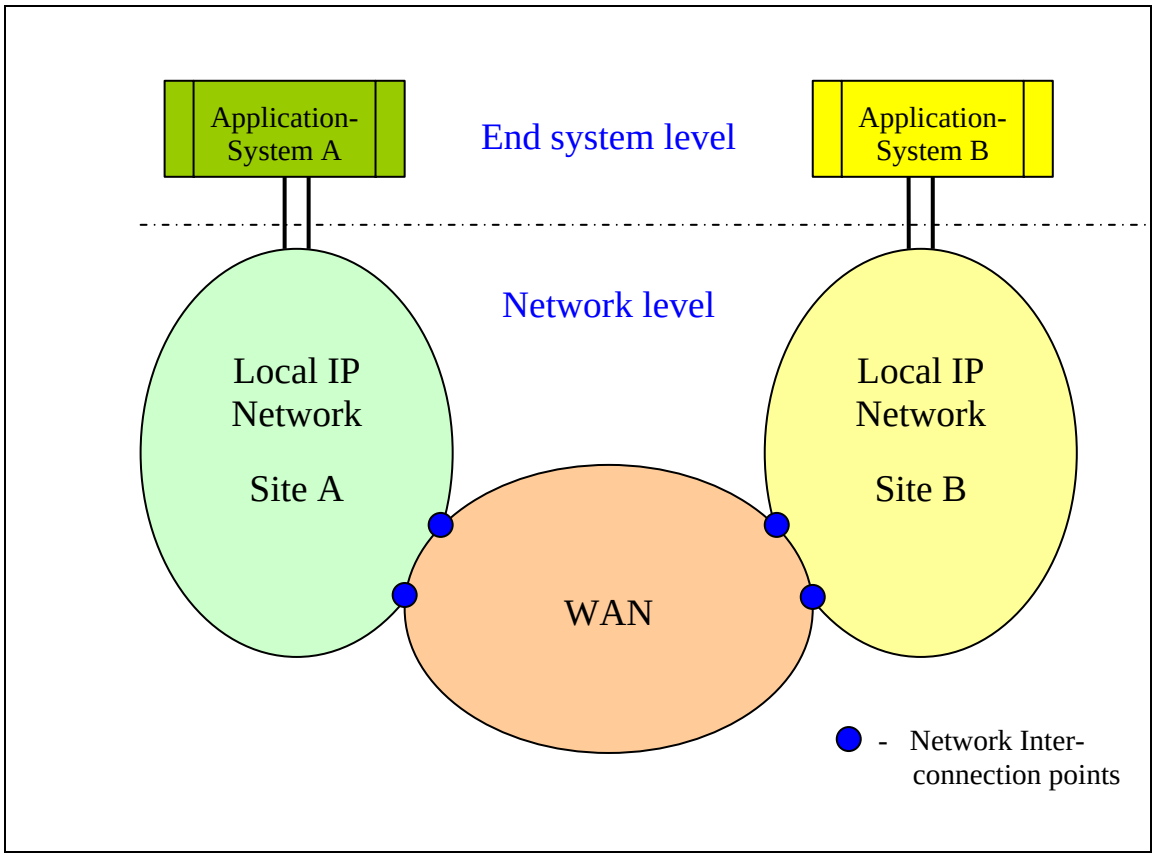

Figure 1: Generic IP Infrastructure

2.1.3 Figure 2 below shows an example of the potential network architecture. Many different variants can exist depending on the network solution adopted by every ANSP.

2.1.4 The "significant points" in the depicted example are:

1. In the National IP segment (Local IP Network Site):

- End system network device (the network device where the application end system is connected).

- Any security device that could be involved in this connection, at national level.

- The entry/exit point in the National IP segment, i.e. ANSPs border router(s).

Note.– Other intermediate network devices could be involved, at national level, in order to provide the required connectivity. These other intermediate points are not considered as significant points in the global view of the end to end connection.

Each ANSP will evaluate if, for internal maintenance, any other intermediate network device should be considered.

The application systems (End systems) could be connected simple or redundant.

2. In the PENS IP segment (WAN):

- The entry/exit point in the PENS IP segment, i.e. PENS border (CE) router(s).

Note.– Other intermediate network devices could be involved, at PENS level, in order to provide the required connectivity. These other intermediate points are not considered as significant points in the global view of the end to end connection. The PENS Service Desk also has to evaluate if, for PENS internal maintenance activities, other devices should be considered.

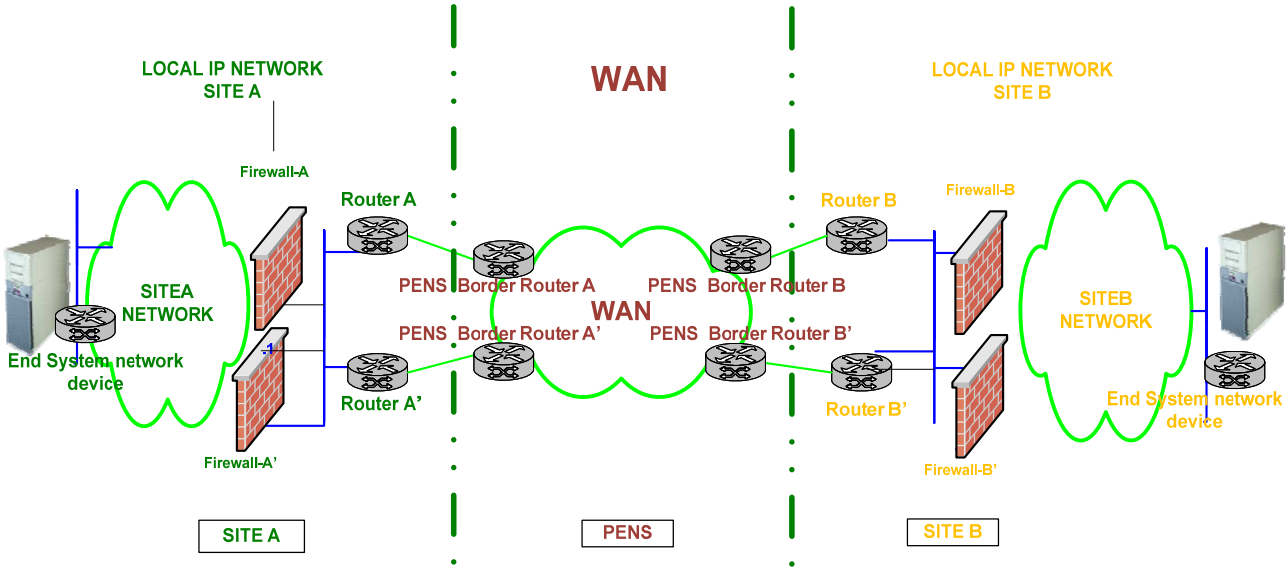

Figure 2: Diagram of a general end to end architecture using PENS

2.2 Generic local IP infrastructure description (Local IP Network Site)

2.2.1 For the IP infrastructure tests the following generic components (see Figure 3) are important:

- LAN (equipment/components) to interconnect the application system in a redundant manner to the Local Router(s)

- Local Router(s)

- Firewall(s)

- Border Router(s)

2.2.2 The responsibility for this infrastructure part is carried by an ANSP. Normally a redundant IP connectivity should be provided.

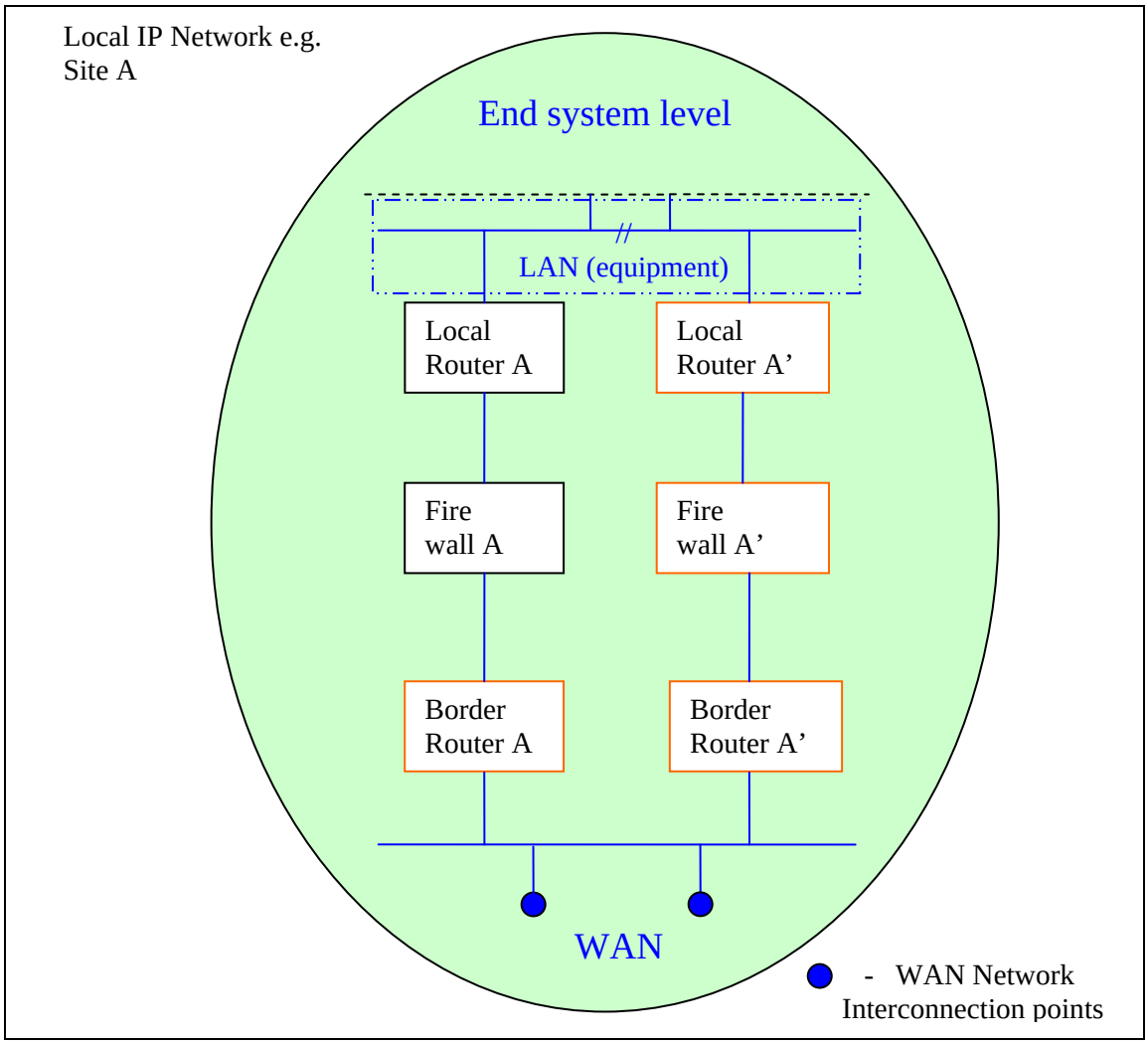

Figure 3: Generic local IP Infrastructure

2.3 Generic WAN IP infrastructure description

2.3.1 For the testing approach the WAN is seen as a black-box providing uninterrupted IP connectivity. Usually the local Network will be connected by two independent physical links (interconnection points) to the WAN (see Figure 4).

2.3.2 The responsibility for this WAN infrastructure is carried by a Telecommunications Service Provider or, in some other cases, by ANSPs' interconnected Networks or by a mixture of both. In all cases the WAN will be seen as one unit (cloud) from the view point of the IP Infrastructure Test.

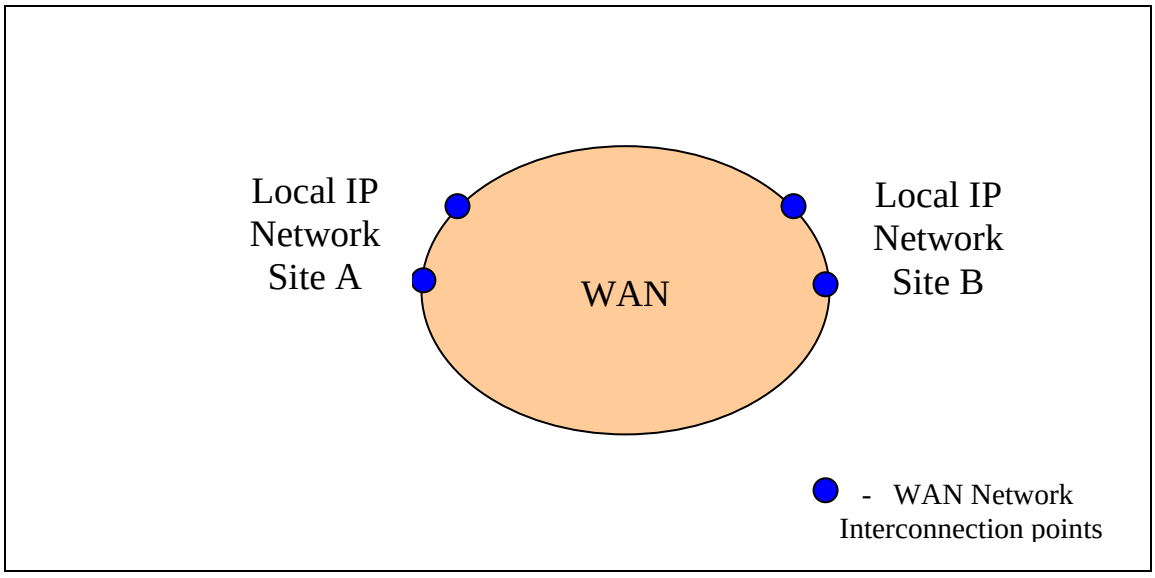

Figure 4: Generic WAN IP Infrastructure

2.4 Levels of influence to be tested

2.4.1 To illustrate the outage (failure) and recovery (switch over) scenarios generic configurations were taken as baseline. Figure 5 shows a generic non-redundant IP Infrastructure, Figure 6 a generic redundant IP Infrastructure and Figure 7 a generic fully redundant IP Infrastructure.

2.4.2 In these configurations 14 potential failing areas were identified. These areas are caused by:

- Outages of LAN components
- Outages of components (routers, fire walls)
- Outage of the connections between the different components

Note.– The outage of the WAN will not be tested; only the loss of connectivity to the WAN. The tests of the WAN itself (features like routing mechanisms, Class of Service, access lists, failure handling, etc.) should be done in special dedicated tests.

2.4.3 All tests have to be performed at both sites.

2.4.4 For all 14 potential failing areas the different test cases are described and test procedures derived. The Test Procedures reflect simulations of physical outages by different means (e.g. disconnection of a cable, switch off of the power supply) and logical outages by 'Disable Port' commands and others.

2.4.5 During the preparation of the tests of a real IP infrastructure the respective generic configuration and the respective test procedures have to be selected and adapted (tailored).

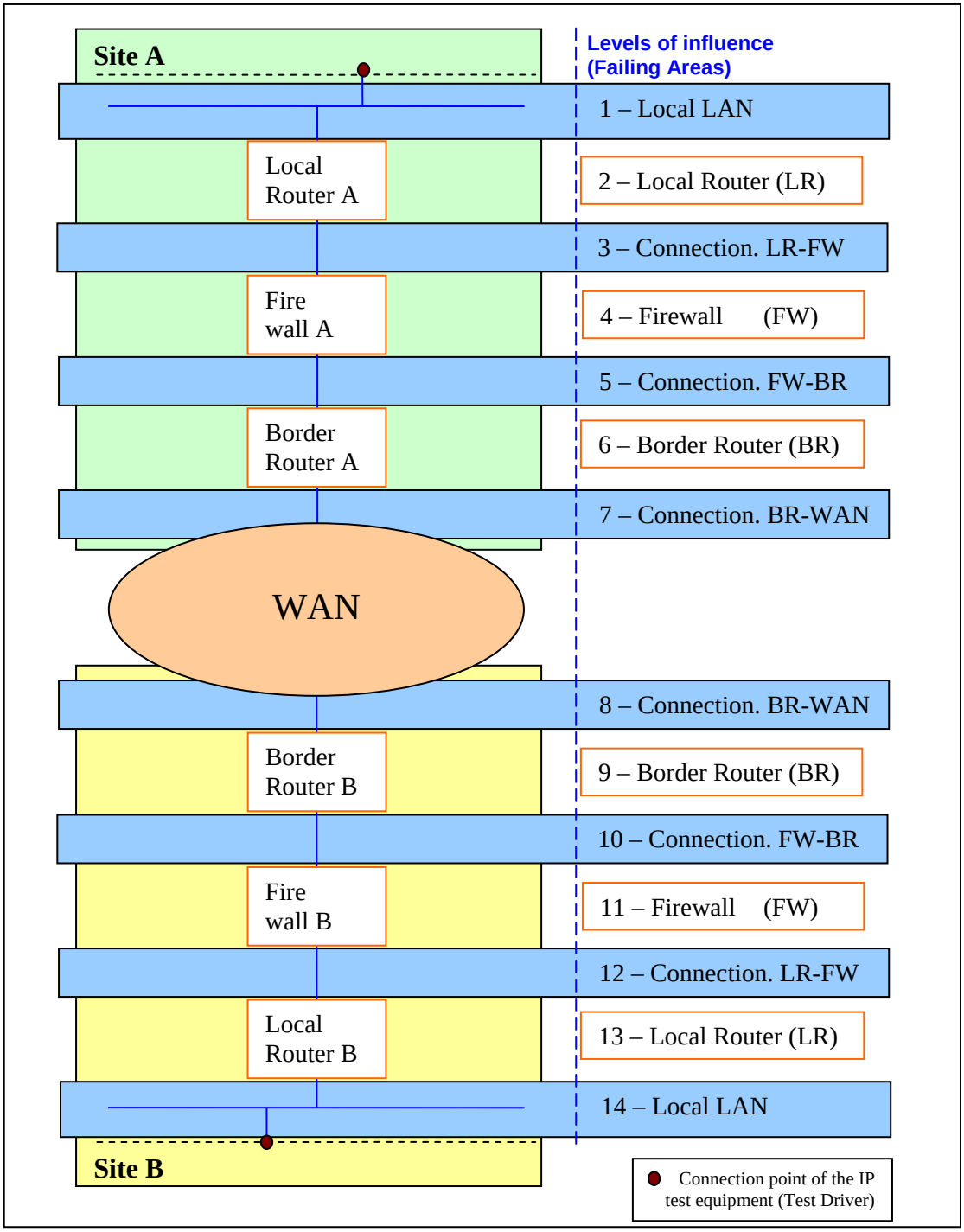

Figure 5: Levels of influence in a generic non-redundant IP Infrastructure

Note.– During preparation and performing of outage tests it should be considered that (part of) the infrastructure under test could be already used by AMHS or other applications in operational use.

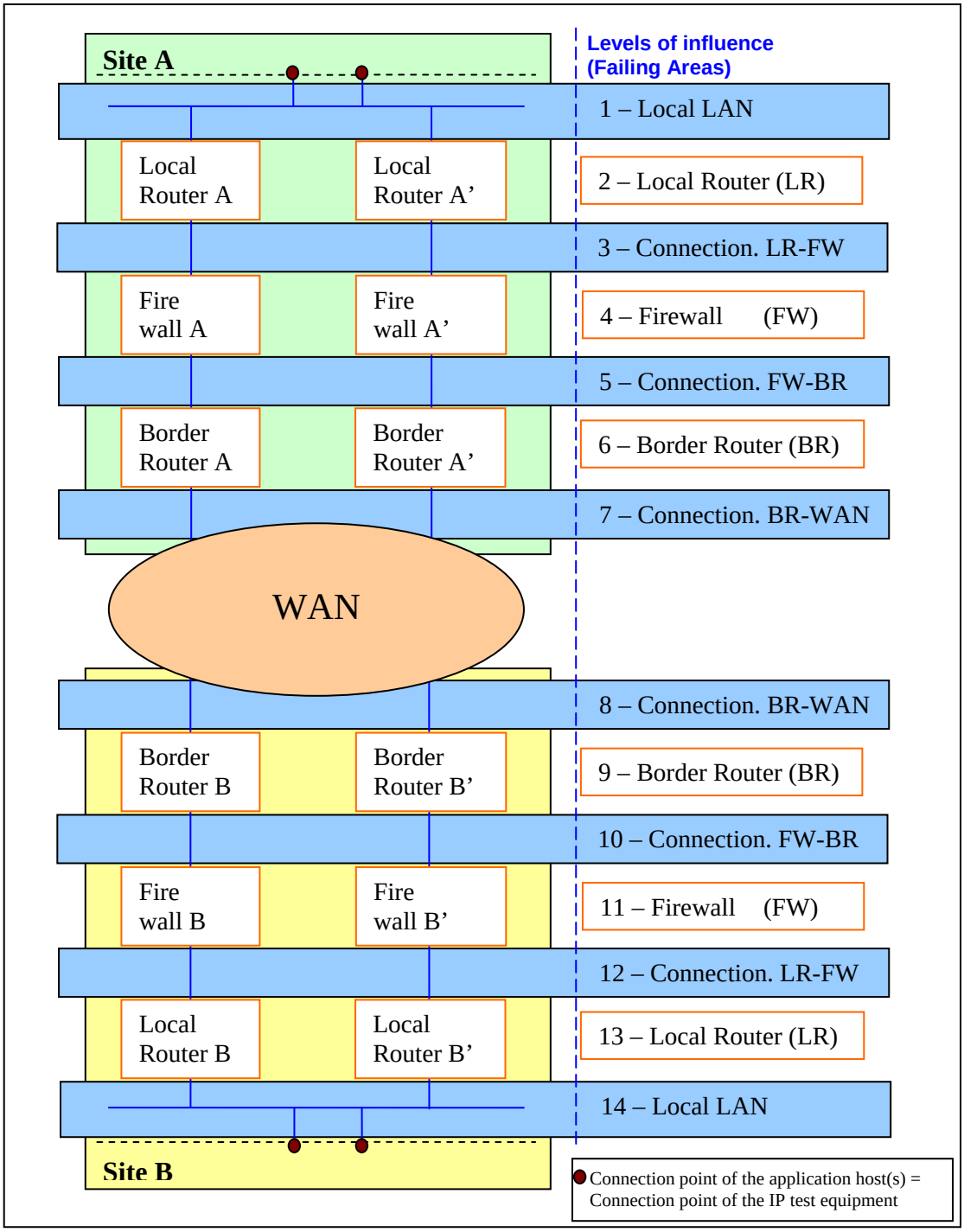

Figure 6: Levels of influence in a generic redundant IP Infrastructure

Note.– During preparation and performing of outage tests it should be considered that (part of) the infrastructure under test could be already used by AMHS or other applications in operational use.

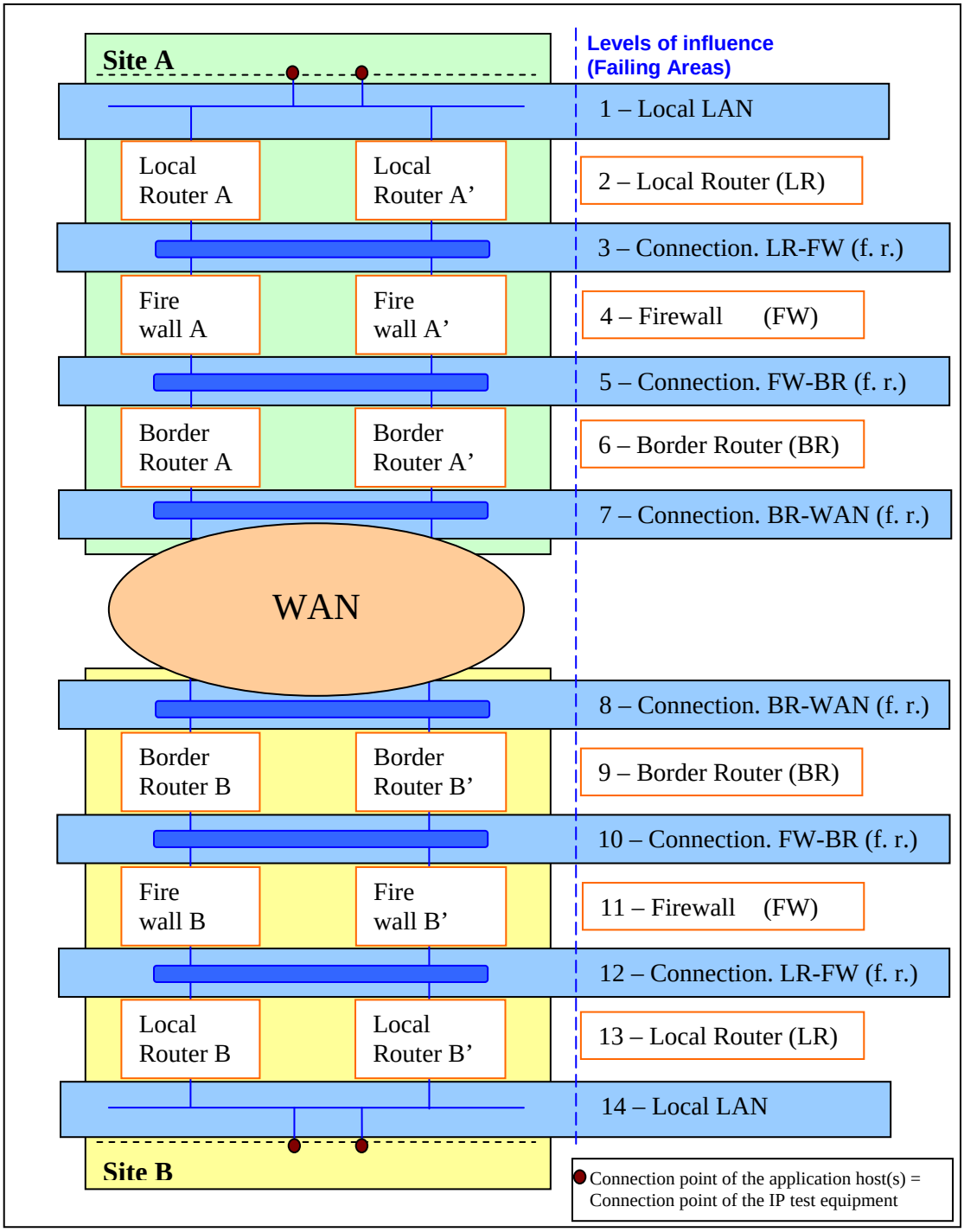

Figure 7: Levels of influence in a generic fully redundant (f. r.) IP Infrastructure

Note.– Fully redundant means that contrary to the 'pure' redundant configuration the connections between the (redundant) infrastructure components in the different failing areas are fully meshed. Therefore the site where the disconnection is initiated is important, due to the different recovery mechanisms which have to come into force.

2.5 IP Test equipment ("Test Drivers")

2.5.1 Connection points of the test drivers

2.5.1.1 In Figure 5 respectively Figure 6 and Figure 7 the connection points of the application hosts are shown. During the IP Infrastructure Test the IP test equipment (test drivers) has to be used at at least one of the same connection points on both sites (see Figure 8).

2.5.1.2 The test drivers (IP test equipment) has to be able to measure, to record the results and log the traffic (e.g. via W*ireshark* traces). Therefore specific programs (tools) for these IP tests should be installed. The IP test equipment should be hardware independent from the application host.

2.5.1.3 The test drivers should be "time synchronised" by adequate means.

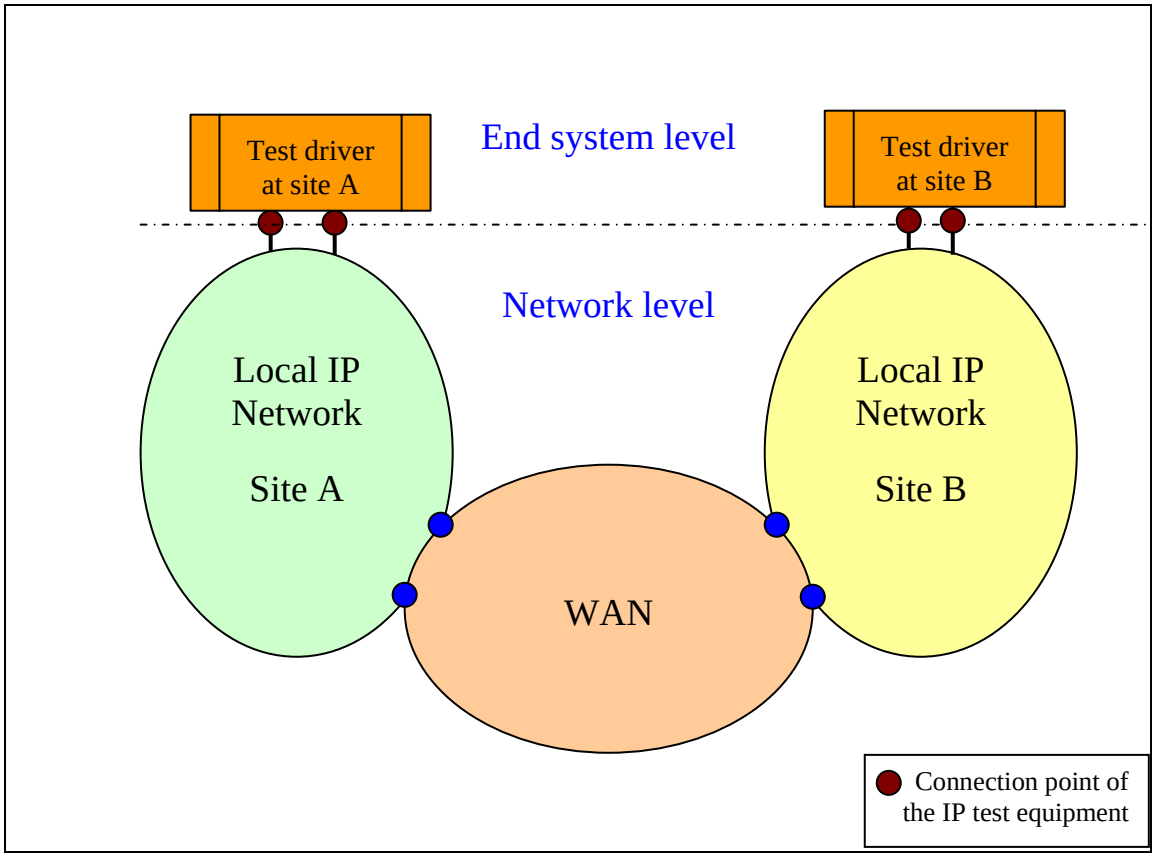

Figure 8: Connection of the test drivers to the IP Infrastructure

2.5.1.4 The Performance check of the requested overall performance (including especially the WAN connectivity) should be measured on base of the future application hardware with specific Tools (e.g. *IPPerf*, *NetIO*, …).

2.5.2 Short description of the tools mentioned above

Note.– Other adequate tools could be used.

2.5.2.1 *Wireshark*

2.5.2.1.1 **Wireshark** is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, in May 2006 the project was renamed Wireshark due to trademark issues.

2.5.2.1.2 **Wireshark** is cross-platform, using the GTK+ widget toolkit to implement its user interface, and using pcap to capture packets; it runs on various Unix-like operating systems including Linux, Mac OS X, BSD, and Solaris, and on Microsoft Windows. There is also a terminal-based (non-GUI) version for Linux called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License.

2.5.2.1.3 **Wireshark** has a rich feature set which includes the following:

- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis
- Powerful display filters
- Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility

2.5.2.2 *IPPerf*

2.5.2.2.1 **Iperf** is a commonly used network testing tool that can create TCP and UDP data streams and measure the throughput of a network that is carrying them. Iperf is a modern tool for network performance measurement written in C++.

2.5.2.2.2 **Iperf** allows the user to set various parameters that can be used for testing a network, or alternately for optimizing or tuning a network. Iperf has a client and server functionality, and can measure the throughput between the two ends, either unidirectonally or bi-directionally. It is open source software and runs on various platforms including Linux, Unix and Windows. It is supported by the National Laboratory for Applied Network Research.

2.5.2.3 *NetIO*

2.5.2.3.1 **NetIO** was designed for the measurement of TCP/IP throughput.

2.5.2.3.2 **NetIO** uses for this measurement 6 different packet sizes for an interval of 10 seconds each. The program is working in all operating system environments. The program is launched by ‘netio –s’ as server (here 192.168.1.1). The data packets are sent to the client under test by ‘netio 192.168.1.1’.

3 IP Infrastructure Configuration and Network Parameters

3.1 Description of the IP infrastructure used in the operational or reference (test) environment

3.1.1 Baseline should be the "target configuration" required for the applications. This configuration has to be used for operations.

3.1.2 In case that the future operational infrastructure can not be used for this kind of testing an equivalent reference test configuration should be established and described.

3.1.3 Figure 9 and Figure 10 show examples how a redundant IP connectivity can be designed. The real configuration and details have to be agreed between the test partners.

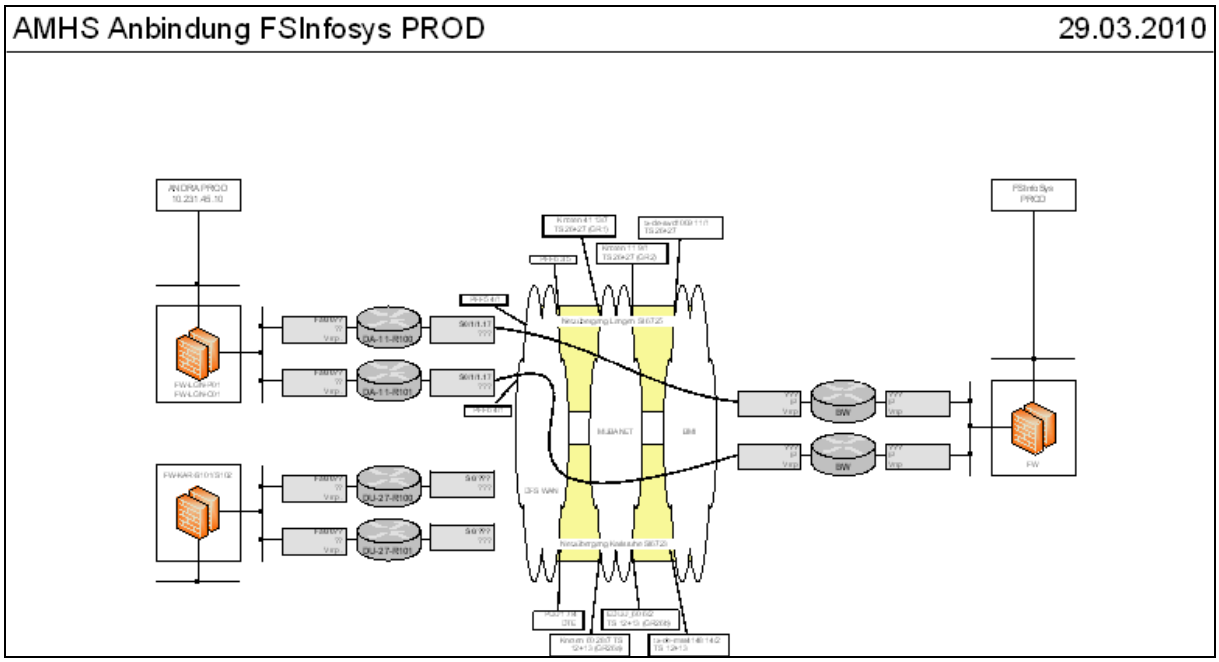

Figure 9: Example of a redundant IP connection (Operational)

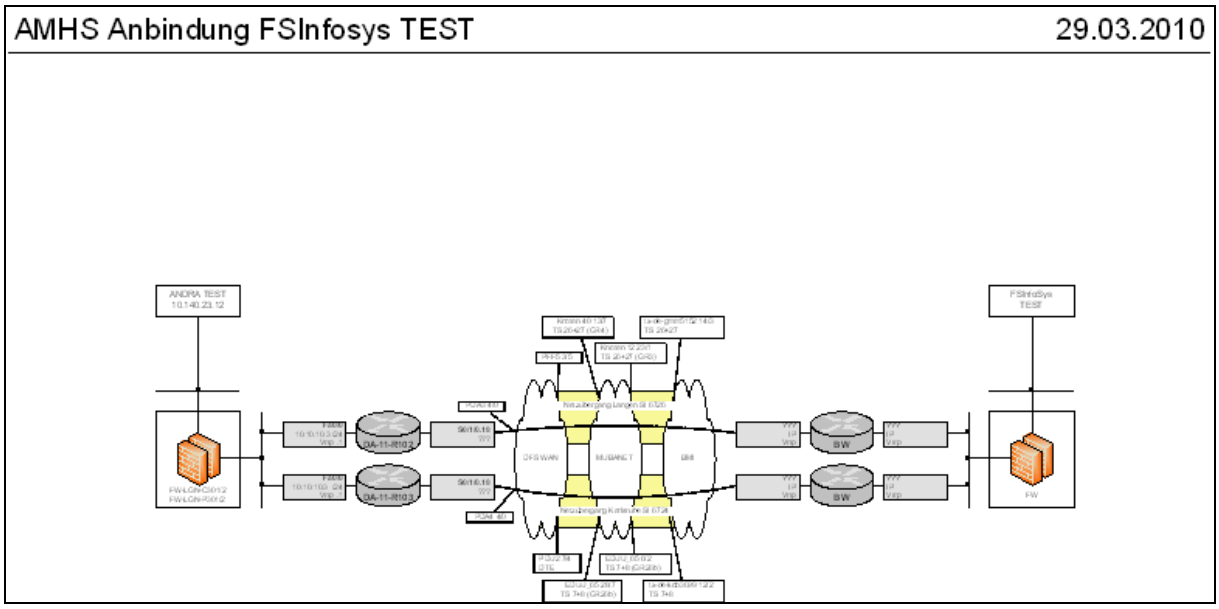

Figure 10: Example of a redundant IP connection (Test)

Note.– For the test report these figures have to be replaced by the real configured and used infrastructure.

3.2 Local IP addresses

3.2.1 Local IPv4 addresses of Test partner A (known at own site, but not published)

3.2.1.1 Due to the local nature of the Local IPv4 Addresses this part could be handled internally. There is no obligation to publish this part. Only those IPv4 Addresses relevant for the WAN Service provider or the other test partner have to be published.

3.2.1.2 In accordance with the recommendations of the former iPAX Task Force (EUROCONTROL) for IPv6 addresses this Section is not relevant for IPv6.

User Name	IP address (IPv4 only)	Remarks

Table 2: Local IP addresses (Test partner A)

Example:

User Name	IP address (IPv4 only)	Remarks
Application host 1	195.66.124.2	AMHS System EDDD
Application host 2	195.66.124.3	AMHS System EDDD

3.2.2 Local IPv4 addresses of Test partner B (known at own site, but not published)

User Name	IP address (IPv4 only)	Remarks

Table 3: Local IP addresses (Test partner B)

Example:

User Name	IP address (IPv4 only)	Remarks
Application host 1	168.22.121.3	AMHS System ABCD
Application host 2	168.22.121.5	AMHS System ABCD

3.3 International IP Addresses (local, LAN, WAN)

3.3.1 International IP addresses of Test partner A

User Name	IP address (IPv6 or IPv4)	Remarks
		Application host
		Local router
		Border router

Table 4: International IP addresses (Test partner A)

Example:

User Name	IP address (IPv6)	Remarks
host_1	2001:4b50:400: … :	Application host
host_2	2001:4b50:400: … :	Application host
router_lflf_1	2001:4b50:400: … :	Local router
router_lflf_2	2001:4b50:400: … :	Local router
router_fr_1	2001:4b50:400: … :	Border router
router_fr_2	2001:4b50:400: … :	Border router

3.3.2 International IP addresses of Test partner B

User Name	IP address (IPv6 or IPv4)	Remarks
		Application host
		Local router
		Border router

Table 5: International IP addresses (Test partner B)

Example:

User Name	IP address (IPv6)	Remarks
host 1	2001:4b50:4**81**: … :	Application host
host 2	2001:4b50:4**81**: … :	Application host
router edll 1	2001:4b50:4**81**: … :	Local router
router edll 2	2001:4b50:4**81**: … :	Local router
router ge 1	2001:4b50:4**81**: … :	Border router
router ge 2	2001:4b50:4**81**: … :	Border router

3.4 IP routing requirements and settings

3.4.1 WAN level

(VRRP Addresses, Routing information, Bandwidth etc.)

3.4.2 Local Level

(VRRP Addresses, Routing information, Bandwidth etc.)

3.4.3 End system setup

(VRRP Addresses, Routing information, Bandwidth etc.)

3.5 Configuration details, defined for the different logical connections in the different elements of the infrastructure (routers, switches …)

3.5.1 Standard templates

- To be added -

3.5.2 Standard parameters and adjustments

- To be added -

3.5.3 Special parameters and adjustments for specific cases if required

- To be added -

3.5.4 Requirements to be fulfilled by the application host (parameters, settings …)

- To be added -

4 IP Test Procedures

4.1 IP reachability tests

The IP reachability to the remote Test Driver is verified using the ICMP ping message (which has to be allowed during these tests). In addition the values measures with the ping command, using 64 bytes, 1024 bytes and 2048 bytes, are logged.

Abnormalities observed during the test or observed in the trace(s) should be reported.

Note.– It is assumed that "Path MTU Discovery" is disabled (Attention: some Firewalls do not forward all ICMP responses) and thereby the "don't fragment bit" is disabled.

It is recommended to check the agreed (direct) routing before the execution of the IP reachability tests especially if several locations could be reached via the same WAN infrastructure in order to avoid unexpected round trip delay results caused by usage of temporary alternate routing paths (usage of the diagnostic tool 'Traceroute').

4.1.1 IPT101 – Ping from Test Driver A to Test Driver B with 64 bytes

IPT101	**Ping from Test Driver A to Test Driver with B 64 bytes**		
Test criteria	This test is successful, if the Test Driver A receives responses on ping messages with 64 bytes.		
Scenario description	Initiate a series of 10 ping messages from Test Driver A to Test Driver B A with size 64 bytes. Verify that responses to the ping messages are received (Test Driver A). Log the results: • Round trip delay (min) _____ • Round trip delay (max) _____ • Average _____ • UTC time test start / end _____/_____ • Packet loss (no. of packets) _____/_____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.1.2 IPT102 – Ping from Test Driver A to Test Driver B with 1024 bytes

IPT102	**Ping from Test Driver A to Test Driver B with 1024 bytes**		
Test criteria	This test is successful, if Test Driver A receives responses on ping messages with 1024 bytes		
Scenario description	Initiate a series of 10 ping messages from Test Driver A to Test Driver B with size 1024 bytes. Verify that responses to the ping messages are received (Test Driver A). Log the results: • Round trip delay (min) _____ • Round trip delay (max) _____ • Average _____ • UTC time test start / end _____/_____ • Packet loss (no. of packets) _____/_____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.1.3 IPT103 – Ping from Test Driver A to Test Driver B with 2048 bytes

IPT103	**Ping from Test Driver A to Test Driver B with 2048 bytes**		
Test criteria	This test is successful, if Test Driver A receives responses on ping messages with 2048 bytes		
Scenario description	Initiate a series of 10 ping messages from Test Driver A to Test Driver B with size 2048 bytes. Verify that responses to the ping messages are received (Test Driver A). Log the results: • Round trip delay (min) _____ • Round trip delay (max) _____ • Average _____ • UTC time test start / end _____/_____ • Note the MTU size of A _____ • Packet loss (no. of packets) _____/_____ *Note.– If the tests fails, the MTU size supported by the network <u>might</u> be the cause. Using pings with smaller size the MTU size can be determined.*		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.1.4 IPT104 – Ping from Test Driver B to Test Driver A with 64 byte

IPT104	**Ping from Test Driver B to Test Driver A with 64 byte**		
Test criteria	This test is successful, if Test Driver B receives responses on ping messages with 64 bytes.		
Scenario description	Initiate a series of 10 ping messages from Test Driver B to Test Driver A with size 64 bytes. Verify that responses to the ping messages are received (at Test Driver B). In particular, verify: • Round trip delay (max) _____ • Round trip delay (min) _____ • Average _____ • UTC time test start / end _____/_____ • Packet loss (no. of packets) _____/_____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.1.5 IPT105 – Ping from Test Driver B to Test Driver A with 1024 byte

IPT105	**Ping from Test Driver B to Test Driver A with 1024 bytes**		
Test criteria	This test is successful, if Test Driver B receives responses on ping messages with 1024 bytes		
Scenario description	Initiate a series of 10 ping messages from Test Driver B to Test Driver A with size 1024 bytes. Verify that responses to the ping messages are received (Test Driver B). Log the results: • Round trip delay (min) _____ • Round trip delay (max) _____ • Average _____ • UTC time test start / end _____/_____ • Packet loss (no. of packets) _____/_____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.1.6 IPT106 – Ping from Test Driver B to Test Driver A with 2048 byte

IPT106	**Ping from Test Driver B to Test Driver A with 2048 bytes**		
Test criteria	This test is successful, if Test Driver B receives responses on ping messages with 2048 bytes		
Scenario description	Initiate a series of 10 ping messages from Test Driver B to Test Driver A with size 2048 bytes. Verify that responses to the ping messages are received (Test Driver B). Log the results: • Round trip delay (min) _____ • Round trip delay (max) _____ • Average _____ • UTC time test start / end _____/_____ • Note the MTU size of B _____ • Packet loss (no. of packets) _____/_____ *Note.– If the tests fails, the MTU size supported by the network <u>might</u> be the cause. Using pings with smaller size the MTU size can be determined.*		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.2 Recovery after Outage (if no redundancy available)

4.2.1 IPT201 – Outage of LAN connection to local router of Test Driver A

IPT201	**Outage of LAN connection to local router of Test Driver A**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the LAN connection(s) to the local router.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Observe that responses to the ping messages are received. Interrupt the LAN connection(s) to the local router of Test Driver A for a period of 3 minutes (e.g. disconnect and connect cables). Verify that responses to the ping messages are received again after the interruption. Measure the recovery time between re-establishment of the connection up to resumption of the ping responses. Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.2.2 IPT202 – Outage of LAN connection to local router of Test Driver B

IPT202	**Outage of LAN connection to local router of Test Driver B**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the LAN connection(s) to the local router.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Observe that responses to the ping messages are received. Interrupt the LAN connection(s) to the local router of Test Driver B for a period of 3 minutes (e.g. disconnect and connect cables). Verify that responses to the ping messages are received again after the interruption. Measure the recovery time between re-establishment of the connection up to resumption of the ping responses. Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.2.3 IPT211 – Outage of the local router of Test Driver A

IPT211	**Outage of the local router of Test Driver A**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the local router.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Switch off the local router of Test Driver A for a period of 3 minutes (e.g. power on/power off). Verify that responses to the ping messages are received again after the interruption. Measure the recovery time between "power on" up to resumption of the ping responses (includes router boot process). Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

Note.– This kind of test has to be performed when the IP infrastructure is established initially. The test should be repeated if a new logical end-to-end connection is configured or added. The disturbance of operational traffic due to testing should be prevented.

4.2.4 IPT212 – Outage of the local router of Test Driver B

IPT212	**Outage of the local router of Test Driver B**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the local router.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Switch off the local router of Test Driver B for a period of 3 minutes (e.g. power on/power off). Verify that responses to the ping messages are received again after the interruption. Measure the recovery time between "power on" up to resumption of the ping responses (includes router boot process). Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

Note.– This kind of test has to be performed when the IP infrastructure is established initially. The test should be repeated if a new logical end-to-end connection is configured or added. The disturbance of operational traffic due to testing should be prevented.

4.2.5 IPT221 – Outage of the connection between local router and firewall at site A

IPT221	**Outage of the connection between local router and firewall at site A**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the connection between local router and firewall.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Observe that responses to the ping messages are received. Interrupt the LAN connection between the local router and the firewall at site A for a period of 3 minutes (e.g. disconnect and connect cable). Verify that responses to the ping messages are received again after the interruption. Measure the recovery time between re-establishment of the connection up to resumption of the ping responses. Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.2.6 IPT222 – Outage of the connection between local router and firewall at site B

IPT222	**Outage of the connection between local router and firewall at site B**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the connection between local router and firewall.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Observe that responses to the ping messages are received. Interrupt the LAN connection between the local router and the firewall at site B for a period of 3 minutes (e.g. disconnect and connect cable). Verify that responses to the ping messages are received again after the interruption. Measure the recovery time between re-establishment of the connection up to resumption of the ping responses. Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.2.7 IPT231 – Outage of the firewall at site A

IPT231	**Outage of the firewall at site A**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the firewall.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Switch off the firewall at site A for a period of 3 minutes (e.g. power on/power off). Verify that responses to the ping messages are received again after the interruption. Measure the recovery time between "power on" up to resumption of the ping responses (includes router boot process). Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

Note.– This kind of test has to be performed when the IP infrastructure is established initially. The test should be repeated if a new logical end-to-end connection is configured or added. The disturbance of operational traffic due to testing should be prevented.

4.2.8 IPT232 – Outage of the firewall at site B

IPT232	**Outage of the firewall at site B**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the firewall.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Switch off the firewall at site B for a period of 3 minutes (e.g. power on/power off). Verify that responses to the ping messages are received again after the interruption. Measure the recovery time between "power on" up to resumption of the ping responses (includes router boot process). Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

Note.– This kind of test has to be performed when the IP infrastructure is established initially. The test should be repeated if a new logical end-to-end connection is configured or added. The disturbance of operational traffic due to testing should be prevented.

4.2.9 IPT241 – Outage of the connection between border router and firewall at site A

IPT241	**Outage of the connection between border router and firewall at site A**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the connection between border router and firewall.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Observe that responses to the ping messages are received. Interrupt the LAN connection between the firewall and border router at site A for a period of 3 minutes (e.g. disconnect and connect cable). Verify that responses to the ping messages are received again after the interruption. Measure the recovery time between re-establishment of the connection up to resumption of the ping responses. Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.2.10 IPT242 – Outage of the connection between border router and firewall at site B

IPT242	**Outage of the connection between border router and firewall at site B**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the connection between border router and firewall.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Observe that responses to the ping messages are received. Interrupt the LAN connection between the firewall and border router at site B for a period of 3 minutes (e.g. disconnect and connect cable). Verify that responses to the ping messages are received again after the interruption. Measure the recovery time between re-establishment of the connection up to resumption of the ping responses. Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.2.11 IPT251 – Outage of the border router at site A

IPT251	**Outage of the border router at site A**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the border router.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Switch off the border router at site A for a period of 3 minutes (e.g. power on/power off). Verify that responses to the ping messages are received again after the interruption. Measure the recovery time between "power on" up to resumption of the ping responses (includes router boot process). Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

Note.– This kind of test has to be performed when the IP infrastructure is established initially. The test should be repeated if a new logical end-to-end connection is configured or added. The disturbance of operational traffic due to testing should be prevented.

4.2.12 IPT252 – Outage of the border router at site B

IPT252	**Outage of the border router at site B**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the border router.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Switch off the border router at site B for a period of 3 minutes (e.g. power on/power off). Verify that responses to the ping messages are received again after the interruption. Measure the recovery time between "power on" up to resumption of the ping responses (includes router boot process). Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

Note.– This kind of test has to be performed when the IP infrastructure is established initially. The test should be repeated if a new logical end-to-end connection is configured or added. The disturbance of operational traffic due to testing should be prevented.

4.2.13 IPT261 – Outage of the connection between border router and WAN at site A

IPT261	**Outage of the connection between border router and WAN at site A**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the connection between border router and WAN.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Observe that responses to the ping messages are received. Interrupt the connection between the border router and WAN at site A for a period of 3 minutes (e.g. disconnect and connect cable, or disable the connection at the WAN side). Verify that responses to the ping messages are received again after the interruption. Measure the recovery time between re-establishment of the connection up to resumption of the ping responses. Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.2.14 IPT262 – Outage of the connection between border router and WAN at site B

IPT262	**Outage of the connection between border router and WAN at site B**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the connection between border router and WAN.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Observe that responses to the ping messages are received. Interrupt the connection between the border router and WAN at site B for a period of 3 minutes (e.g. disconnect and connect cable, or disable the connection at the WAN side). Verify that responses to the ping messages are received again after the interruption. Measure the recovery time between re-establishment of the connection up to resumption of the ping responses. Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.3 Redundancy Recovery

4.3.1 IPT301 – Outage of LAN connection to one of the local routers of Test Driver A

IPT301	**Outage of LAN connection to one of the local routers of Test Driver A**		
Test criteria	This test is successful, if the outage of the LAN connection to one of the local routers has no or temporary influence on the end-to-end IP connectivity.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Observe that responses to the ping messages are received. Interrupt the LAN connection to the "active" local router of Test Driver A (e.g. disconnect LAN cable at router). Verify that responses to the ping messages are received. Note the recovery time (period of no response on ping messages): • Recovery time (if any) at Test Driver A: _____ • Recovery time (if any) at Test Driver B: _____ • UTC time test start / end _____/_____ Re-connect the cable and wait 3 minutes. Observe that responses to the ping messages are received. Interrupt the LAN connection to the other local router of Test Driver A (e.g. disconnect LAN cable at router). Verify that responses to the ping messages are received. Note the recovery time (period of no response on ping messages): • Recovery time (if any) at Test Driver A: _____ • Recovery time (if any) at Test Driver B: _____ • UTC time test start / end _____/_____ Re-connect the cable. Observe that responses to the ping messages are received.		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.3.2 IPT302 – Outage of LAN connection to one of the local routers of Test Driver B

IPT302	**Outage of LAN connection to one of the local routers of Test Driver B**		
Test criteria	This test is successful, if the outage of the LAN connection to one of the local routers has no or temporary influence on the end-to-end IP connectivity.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Observe that responses to the ping messages are received. Interrupt the LAN connection to the "active" local router of Test Driver B (e.g. disconnect LAN cable at router). Verify that responses to the ping messages are received. Note the recovery time (period of no response on ping messages): • Recovery time (if any) at Test Driver A: _____ • Recovery time (if any) at Test Driver B: _____ • UTC time test start / end _____/_____ Re-connect the cable and wait 3 minutes. Observe that responses to the ping messages are received. Interrupt the LAN connection to the other local router of Test Driver B (e.g. disconnect LAN cable at router). Verify that responses to the ping messages are received. Note the recovery time (period of no response on ping messages): • Recovery time (if any) at Test Driver A: _____ • Recovery time (if any) at Test Driver B: _____ • UTC time test start / end _____/_____ Re-connect the cable. Observe that responses to the ping messages are received.		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.3.3 IPT311 – Outage of one of the local routers of Test Driver A

IPT311	**Outage of one of the local routers of Test Driver A**		
Test criteria	This test is successful, if the outage of one of the local routers has no or temporary influence on the end-to-end IP connectivity.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Observe that responses to the ping messages are received. Switch off the "active" local router (primary Gateway) of Test Driver A (e.g. power off). Verify that responses to the ping messages are received. Note the recovery time (period of no response on ping messages): • Recovery time (if any) at Test Driver A: _____ • Recovery time (if any) at Test Driver B: _____ • UTC time test start / end _____/_____ Switch the router on again and wait 3 minutes. Observe that responses to the ping messages are received. Switch off the other local router of Test Driver A (e.g. power off). Verify that responses to the ping messages are received. Note the recovery time (period of no response on ping messages): • Recovery time (if any) at Test Driver A: _____ • Recovery time (if any) at Test Driver B: _____ • UTC time test start / end _____/_____ Switch the router on again and wait 3 minutes. Observe that responses to the ping messages are received.		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

Note.– This kind of test has to be performed when the IP infrastructure is established initially. The test should be repeated if a new logical end-to-end connection is configured or added. The disturbance of operational traffic due to testing should be prevented.

4.3.4 IPT312 – Outage of one of the local routers of Test Driver B

IPT312	**Outage of one of the local routers of Test Driver B**		
Test criteria	This test is successful, if the outage of one of the local routers has no or temporary influence on the end-to-end IP connectivity.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Observe that responses to the ping messages are received. Switch off the "active" local routers (primary Gateway) of Test Driver B (e.g. power off). Verify that responses to the ping messages are received. Note the recovery time (period of no response on ping messages): • Recovery time (if any) at Test Driver A: _____ • Recovery time (if any) at Test Driver B: _____ • UTC time test start / end _____/_____ Switch the router on again and wait 3 minutes. Observe that responses to the ping messages are received. Switch off the other local router of Test Driver B (e.g. power off). Verify that responses to the ping messages are received. Note the recovery time (period of no response on ping messages): • Recovery time (if any) at Test Driver A: _____ • Recovery time (if any) at Test Driver B: _____ • UTC time test start / end _____/_____ Switch the router on again and wait 3 minutes. Observe that responses to the ping messages are received.		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

Note.– This kind of test has to be performed when the IP infrastructure is established initially. The test should be repeated if a new logical end-to-end connection is configured or added. The disturbance of operational traffic due to testing should be prevented.

4.3.5 IPT321 – Outage of the connection between a local router and firewall at site A

IPT321	**Outage of the connection between a local router and firewall at site A**		
Test criteria	This test is successful, if the outage of the connection between a local router and firewall has no or temporary influence on the end-to-end IP connectivity. *Note.– Perform Case II only if the LAN is fully redundant.*		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Observe that responses to the ping messages are received. Interrupt the LAN connection between a local router and the firewall at site A for a period of 3 minutes (e.g. disconnect and connect cable): Case I: at the router Case II: at the firewall if the LAN is fully redundant. Verify that responses to the ping messages are received again after the interruption. Note the recovery time (period of no response on ping messages): Log the results: Case I Case II • Recovery time at Test Driver A: _____ _____ • Recovery time at Test Driver B: _____ _____ Interrupt the LAN connection between the other local router and the firewall at site A for a period of 3 minutes (e.g. disconnect and connect cable): Case I: at the router Case II: at the firewall if the LAN is fully redundant. Verify that responses to the ping messages are received again after the interruption. Note the recovery time (period of no response on ping messages): Log the results: Case I Case II • Recovery time at Test Driver A: _____ _____ • Recovery time at Test Driver B: _____ _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.3.6 IPT322 – Outage of the connection between a local router and firewall at site B

IPT322	**Outage of the connection between a local router and firewall at site B**		
Test criteria	This test is successful, if the outage of the connection between a local router and firewall has no or temporary influence on the end-to-end IP connectivity. *Note.– Perform Case II only if the LAN is fully redundant.*		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Observe that responses to the ping messages are received. Interrupt the LAN connection between a local router and the firewall at site B for a period of 3 minutes (e.g. disconnect and connect cable): Case I: at the router Case II: at the firewall if the LAN is fully redundant. Verify that responses to the ping messages are received again after the interruption. Note the recovery time (period of no response on ping messages): Log the results: Case I Case II • Recovery time at Test Driver A: _____ _____ • Recovery time at Test Driver B: _____ _____ Interrupt the LAN connection between the other local router and the firewall at site B for a period of 3 minutes (e.g. disconnect and connect cable): Case I: at the router Case II: at the firewall if the LAN is fully redundant. Verify that responses to the ping messages are received again after the interruption. Note the recovery time (period of no response on ping messages): Log the results: Case I Case II • Recovery time at Test Driver A: _____ _____ • Recovery time at Test Driver B: _____ _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.3.7 IPT331 – Outage of the firewall at site A

IPT331	**Outage of the firewall at site A**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the firewall.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Switch off one of the firewalls at site A for a period of 3 minutes (e.g. power on/power off). Verify that responses to the ping messages are received again after the interruption. Note the recovery time (period of no response on ping messages): Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____ Switch off the other firewall at site A for a period of 3 minutes (e.g. power on/power off). Verify that responses to the ping messages are received again after the interruption. Note the recovery time (period of no response on ping messages): Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

Note.– This kind of test has to be performed when the IP infrastructure is established initially. The test should be repeated if a new logical end-to-end connection is configured or added. The disturbance of operational traffic due to testing should be prevented.

4.3.8 IPT332 – Outage of the firewall at site B

IPT332	**Outage of the firewall at site B**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the firewall.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Switch off one of the firewalls at site B for a period of 3 minutes (e.g. power on/power off). Verify that responses to the ping messages are received again after the interruption. Note the recovery time (period of no response on ping messages): Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____ Switch off the other firewall at site B for a period of 3 minutes (e.g. power on/power off). Verify that responses to the ping messages are received again after the interruption. Note the recovery time (period of no response on ping messages): Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

Note.– This kind of test has to be performed when the IP infrastructure is established initially. The test should be repeated if a new logical end-to-end connection is configured or added. The disturbance of operational traffic due to testing should be prevented.

4.3.9 IPT341 – Outage of the connection between border router and firewall at site A

IPT341	**Outage of the connection between border router and firewall at site A**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the connection between border router and firewall.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Observe that responses to the ping messages are received. Interrupt the LAN connection between a firewall and border router at site A for a period of 3 minutes (e.g. disconnect and connect cable): Case I: at the router Case II: at the firewall if the LAN is fully redundant. Verify that responses to the ping messages are received again after the interruption. Note the recovery time (period of no response on ping messages): Log the results: Case I Case II • Recovery time at Test Driver A: _____ _____ • Recovery time at Test Driver B: _____ _____ Interrupt the LAN connection between the other firewall and border router at site A for a period of 3 minutes (e.g. disconnect and connect cable): Case I: at the router Case II: at the firewall if the LAN is fully redundant. Verify that responses to the ping messages are received again after the interruption. Note the recovery time (period of no response on ping messages): Log the results: Case I Case II • Recovery time at Test Driver A: _____ _____ • Recovery time at Test Driver B: _____ _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.3.10 IPT342 – Outage of the connection between border router and firewall at site B

IPT342	**Outage of the connection between border router and firewall at site B**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the connection between border router and firewall.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Observe that responses to the ping messages are received. Interrupt the LAN connection between a firewall and border router at site B for a period of 3 minutes (e.g. disconnect and connect cable): Case I: at the router Case II: at the firewall if the LAN is fully redundant. Verify that responses to the ping messages are received again after the interruption. Note the recovery time (period of no response on ping messages): Log the results: Case I Case II • Recovery time at Test Driver A: _____ _____ • Recovery time at Test Driver B: _____ _____ Interrupt the LAN connection between the other firewall and border router at site B for a period of 3 minutes (e.g. disconnect and connect cable): Case I: at the router Case II: at the firewall if the LAN is fully redundant. Verify that responses to the ping messages are received again after the interruption. Note the recovery time (period of no response on ping messages): Log the results: Case I Case II • Recovery time at Test Driver A: _____ _____ • Recovery time at Test Driver B: _____ _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.3.11 IPT351 – Outage of the border router at site A

IPT351	**Outage of the border router at site A**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the border router.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Switch off a border router (primary Gateway) at site A for a period of 3 minutes (e.g. power on/power off). Verify that responses to the ping messages are received again after the interruption. Note the recovery time (period of no response on ping messages): Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____ Switch off the other border router at site A for a period of 3 minutes (e.g. power on/power off). Verify that responses to the ping messages are received again after the interruption. Note the recovery time (period of no response on ping messages): Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

Note.– This kind of test has to be performed when the IP infrastructure is established initially. The test should be repeated if a new logical end-to-end connection is configured or added. The disturbance of operational traffic due to testing should be prevented.

4.3.12 IPT352 – Outage of the border router at site B

IPT352	**Outage of the border router at site B**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the border router.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Switch off a border router (primary Gateway) at site B for a period of 3 minutes (e.g. power on/power off). Verify that responses to the ping messages are received again after the interruption. Note the recovery time (period of no response on ping messages): Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____ Switch off the other border router at site B for a period of 3 minutes (e.g. power on/power off). Verify that responses to the ping messages are received again after the interruption. Note the recovery time (period of no response on ping messages): Log the results: • Recovery time at Test Driver A: _____ • Recovery time at Test Driver B: _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

Note.– This kind of test has to be performed when the IP infrastructure is established initially. The test should be repeated if a new logical end-to-end connection is configured or added. The disturbance of operational traffic due to testing should be prevented.

4.3.13 IPT361 – Outage of the connection between border router and WAN at site A

IPT361	**Outage of the connection between border router and WAN at site A.**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the connection between border router and WAN.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Observe that responses to the ping messages are received. Interrupt the connection between a border router and WAN at site A for a period of 3 minutes (e.g. disconnect and connect cable, or disable the connection at the WAN side): Case I: at the router Case II: at the WAN if the connection is fully redundant. Verify that responses to the ping messages are received again after the interruption. Note the recovery time (period of no response on ping messages): Log the results: Case I Case II • Recovery time at Test Driver A: _____ _____ • Recovery time at Test Driver B: _____ _____ Interrupt the connection between the other border router and WAN at site A for a period of 3 minutes (e.g. disconnect and connect cable, or disable the connection at the WAN side): Case I: at the router Case II: at the WAN if the connection is fully redundant. Verify that responses to the ping messages are received again after the interruption. Note the recovery time (period of no response on ping messages): Log the results: Case I Case II • Recovery time at Test Driver A: _____ _____ • Recovery time at Test Driver B: _____ _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.3.14 IPT362 – Outage of the connection between border router and WAN at site B

IPT362	**Outage of the connection between border router and WAN at site B**		
Test criteria	This test is successful, if the end-to-end IP connectivity is automatically recovered after a temporary outage of the connection between border router and WAN.		
Scenario description	Initiate permanent ping messages from Test Driver A to Test Driver B and from Test Driver B to Test Driver A. Observe that responses to the ping messages are received. Interrupt the connection between a border router and WAN at site B for a period of 3 minutes (e.g. disconnect and connect cable, or disable the connection at the WAN side): Case I: at the router Case II: at the WAN if the connection is fully redundant. Verify that responses to the ping messages are received again after the interruption. Note the recovery time (period of no response on ping messages): Log the results: Case I Case II • Recovery time at Test Driver A: _____ _____ • Recovery time at Test Driver B: _____ _____ Interrupt the connection between the other border router and WAN at site B for a period of 3 minutes (e.g. disconnect and connect cable, or disable the connection at the WAN side): Case I: at the router Case II: at the WAN if the connection is fully redundant. Verify that responses to the ping messages are received again after the interruption. Note the recovery time (period of no response on ping messages): Log the results: Case I Case II • Recovery time at Test Driver A: _____ _____ • Recovery time at Test Driver B: _____ _____		
Test result:	**PASS**	**FAILED**	**INCONCLUSIVE**

4.4 Performance Tests

Performance tests (measurement of TCP/IP throughput) should be executed after successful completion of the IP Infrastructure Tests in the application environment foreseen for going into operation.

If possible the performance test tools mentioned in Section 2.5.2 (e.g. NetIO) should run at the application hosts in order to ensure that the performance is measured under real physical conditions (including the connections between application host and IP infrastructure). Otherwise the tests should be performed by the Test Driver system.

The respective tool has to be started using the same IP Port which is used by the application (AMHS e.g. 102). The results have to be logged and should be included in the test report of the IP Infrastructure Tests.

Attachment A: Change Control Mechanism of the IP Infrastructure Test Guidelines

A.0.1 The change control mechanism provides two categories:

- Defect Report (DR), and
- Change Proposal (CP)

A.0.2 Proposals to introduce changes to the IP Infrastructure Test Guidelines document itself may arise from users, implementers or manufacturers.

A.0.3 The procedure for submission and processing of a Defect Report (DR) or a Change Proposal (CP) involves the following steps:

A.1 Procedure for Defect Report (DR)

A.1.1 A problem is detected, which is reflected in the IP Infrastructure Test Guidelines and may be attributed to implement procedures and/or inconsistencies in this document.

A.1.2 The problem is reported to the Rapporteur of the AFSG Planning Group (PG), by submission of a defect report (DR). A standard reporting format is used (see attached template in A.3).

A.1.3 The Rapporteur assigns a number and priority to the defect report and introduces it to the agenda of an upcoming meeting of the PG. If necessary, he refers to the Operations Group (OG) Rapporteur.

A.1.4 The PG evaluates the report and either adopts it as a working item or rejects it. The party, which submitted the defect report, is notified accordingly.

A.1.5 Experts of the PG are assigned to the problem when adopted (Status: accepted) and milestone dates are set. Outside expertise may be invited to participate, as appropriate.

A.1.6 The PG develops proposals for resolving the problem and submits them to the AFSG for approval.

A.1.7 The AFSG approves or rejects the presented proposals. In case of the latter, the subject is referred back to the PG (step A.1.5) or discarded.

A.1.8 The PG drafts appropriate text for amendment of the IP Infrastructure Test Guidelines and submits it to the AFSG for approval.

A.1.9 The AFSG approves or rejects the proposed material. In case of the latter, the subject is referred back to the PG (step A.1.8).

A.1.10 Solutions are implemented.

Note.– Steps A.1.6 and A.1.8 may run in parallel.

A.2 Procedure for Change Proposal (CP)

A.2.1 The same structured procedure, with the exception of steps (A.1.6) and (A.1.7) applies in case of proposed enhancements to the IP Infrastructure Test Guidelines or inconsistencies with relevant existing documentation.

A.2.2 In this case, a change proposal (CP) should be submitted to the PG. The format of the CP is similar to that of the DR.

A.3 Template for Defect Reports / Change Proposals

TEMPLATE FOR DEFECT REPORTS / CHANGE PROPOSALS

DR_____ **CP_____**

Title:	Short, indicative textual name
Reference:	Number assigned by the PG Rapporteur
Originator reference:	Provided by the originator
Submission date:	
Submitting State/Organisation:	
Author:	
Contact Information:	e-mail, fax, telephone and postal address
Experts involved:	
Status:	Assigned by the PG Rapporteur
Priority:	Assigned by the PG Rapporteur
Document reference:	Affected section(s) of the IP Infrastructure Test Guidelines
Description of defect:	Nature of the problem in detail Reason(s) for requesting changes
Assigned expert(s):	
Task history:	Working Papers and Information Papers Produced on the subject
Proposed solution:	Including amendments to the text, if feasible

DR/CP STATUS control sheet				
Event	**Date**	**Status**		**Remark**
DR or CP received submission date		Set to submitted		
discussion at PG/ ...		Set to accepted	Set to rejected	
Date for development of proposals/ solutions				Responsible:
discussion at PG/ ...		Set to resolved		
presentation to AFSG/ ...		Set to adopted	Set to rejected	
Date for development of amendment to the IP Infrastructure Test Guidelines				Responsible:
discussion at PG/		Set to approved		
presentation to AFSG/ ...		Set to approved for application		
Additional DATES and comments				

END of document