



# An Intelligent Resilient Framework at a University Campus

## Best Practice Document

Produced by the CESNET-led working group  
on network monitoring

Authors: Pavel Kislinger (VUT), Vladimír Záhořík (VUT)

October 2015

© CESNET, 2015    © GÉANT, 2015. All rights reserved.

Document No: GN3-CBPD123  
Version / date: V1.0, 09 October 2015  
Original language : English  
Original title: “ Intelligent Resilient Framework at University Campus ”  
Original version / date: V1.0, May 2015  
Contact: [kislinger@cis.vutbr.cz](mailto:kislinger@cis.vutbr.cz), [zahorik@cis.vutbr.cz](mailto:zahorik@cis.vutbr.cz)

CESNET is responsible for the contents of this document. The document was developed by a CESNET-led working group on network monitoring as part of a joint-venture project within the higher-education sector in the Czech Republic.

Parts of the report may be freely copied, unaltered, provided that the original source is acknowledged and copyright preserved.

The research leading to these results has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).

## Table of Contents

|       |                                |    |
|-------|--------------------------------|----|
| 1     | Executive Summary              | 1  |
| 2     | The original network topology  | 3  |
| 3     | Topology changes               | 5  |
| 3.1   | Physical topology              | 5  |
| 3.2   | Logical topology               | 6  |
| 4     | IRF configuration              | 7  |
| 4.1   | IRF from two devices           | 7  |
| 4.2   | IRF from three or more devices | 8  |
| 4.3   | ISSU update                    | 9  |
| 4.3.1 | Software redistribution        | 10 |
| 4.3.2 | Update procedure               | 10 |
| 4.3.3 | Two node Link Aggregation      | 11 |
| 5     | Conclusion                     | 12 |
|       | References                     | 13 |
|       | Glossary                       | 14 |

## Table of Figures

|             |                             |   |
|-------------|-----------------------------|---|
| Figure 1.1: | IRF using link aggregation  | 1 |
| Figure 2.1: | Original network topology   | 3 |
| Figure 3.1: | Revised network topology    | 5 |
| Figure 3.2: | Simplified network topology | 6 |

# 1 Executive Summary

Intelligent Resilient Framework (IRF) is a network virtualization technology developed by HP (originally by 3Com) and it is available on current models of HP Ethernet switches and routers based on comware software. The basic idea of this technology is to interconnect multiple network devices through its interface ports to form a single virtual chassis with one management. IRF can be formed from 2–9 physical devices arranged in a ring topology. IRF can use physical 10, 40, 100-Gigabit Ethernet interfaces, whether they are copper or optical.

Two or more ports on different physical devices can also create a single logical connection. This logical connection uses the standard link-aggregation protocols (IEEE 802.1ax, IEEE 802.1aq or the previous IEEE 802.3ad). Link-aggregation technology is the basic building block of resiliency in IRF. It provides connection failover for a basic L2 switch, as well as for a server, because the logical connection is not terminated on a single physical device but on two physical devices.

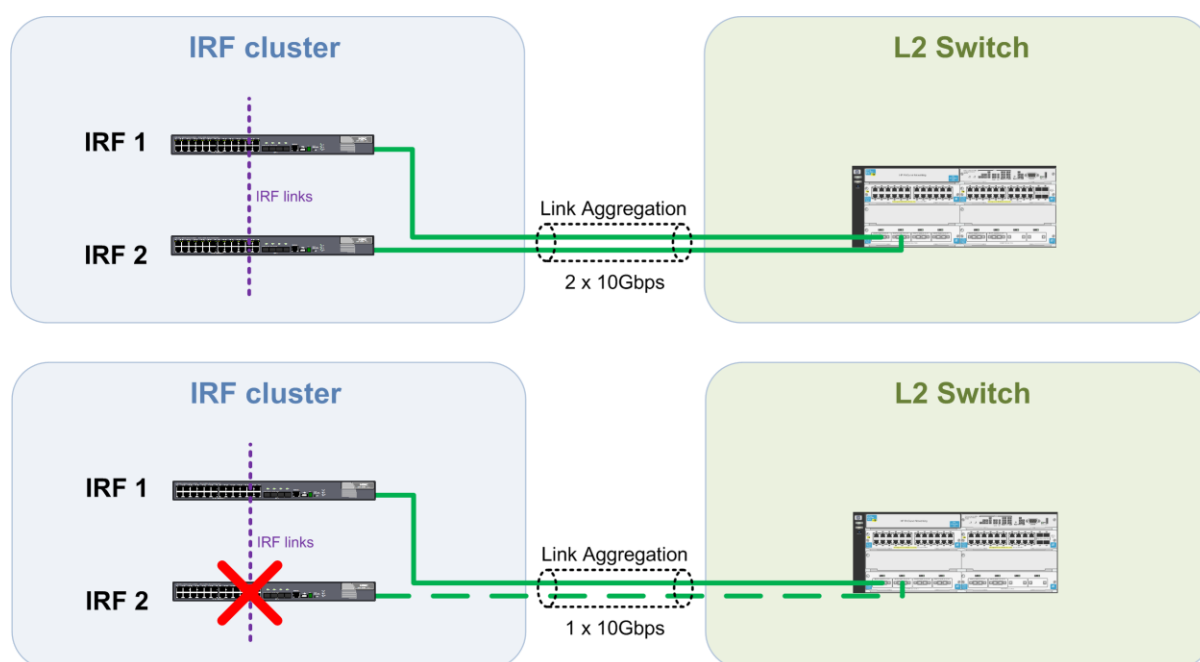


Figure 1.1: IRF using link aggregation

IRF is a technology that can simplify the network topology of data centres and campus networks, eliminating the need for a dedicated aggregation layer and providing more direct, higher capacity connections between users and network resources. HP is not the only vendor to offer a network virtualization technology. Among the best known technologies for virtual switching include: Cisco – Virtual Switching System (VSS), Juniper – Virtual Chassis, Allied Telesis – Virtual Chassis Stacking (VCStack), Huawei – Intelligent Stacking (IStack), HP – Intelligent Resilient Framework (IRF), and more. These technologies are conceptually very similar but they are not mutually compatible.

In most installations, the virtual chassis is typically formed of two physical devices. This document focuses on an unusual setup from this point of view. The document describes a way of how to migrate a traditional STP-based campus network to an IRF virtual chassis using long-range fibre between four distant locations.

The first part describes the original state of the computer network and the main disadvantages of this set up. The next sections explain how the topology changes after deploying a virtual chassis. The third part is devoted to a specific configuration of network devices and to the preparation required before connecting individual parts of the virtual chassis. The final section presents the summary of the benefits and pitfalls of the technologies used and the operating statistics both before and after deployment.

## 2 The original network topology

The student dormitory network at the Brno University of Technology (BUT) consists of four localities in the north of the city of Brno, Czech Republic. Individual sites are connected via fibre-optic to the University backbone network.

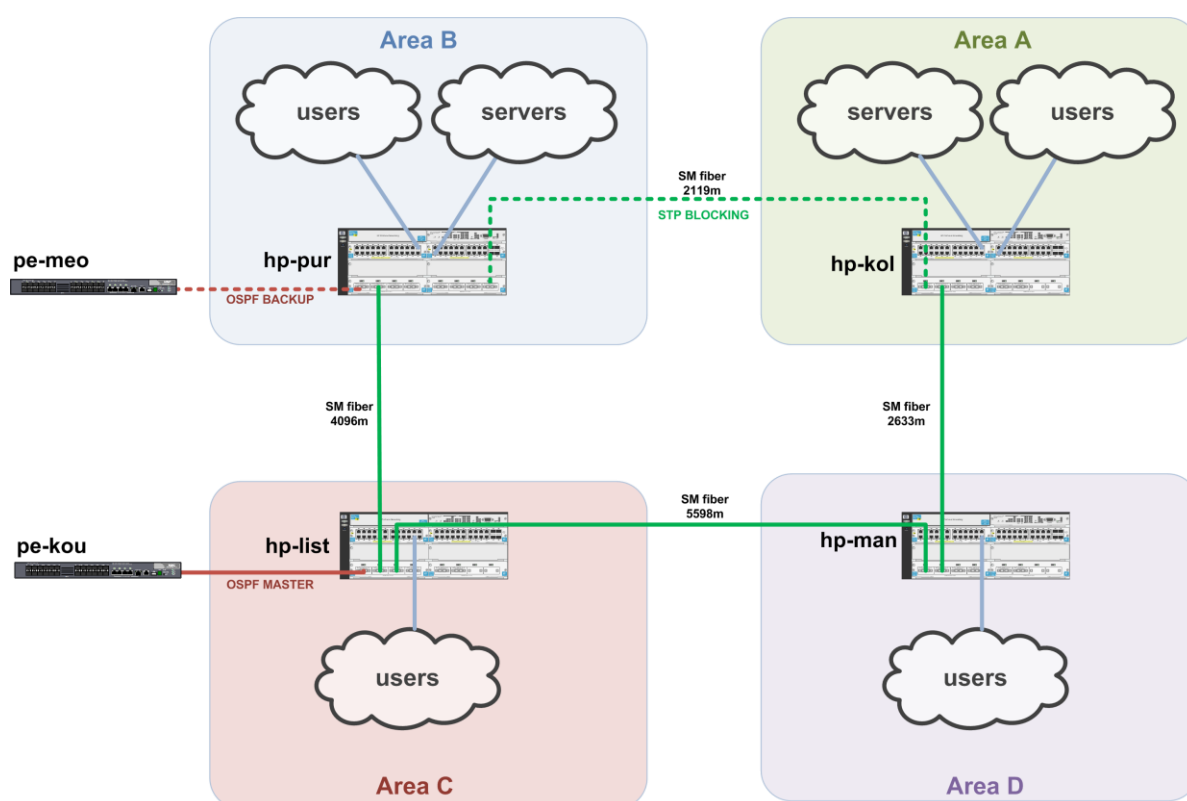


Figure 2.1: Original network topology

IPv4 and IPv6 connectivity is ensured by the L3 router HP 5406 in each area. Routers are connected to the university OSPF Area (OSPfv3 for IPv6). The student dormitory network forms a ring topology with two uplink connection to the whole university backbone network. One of these uplinks is always disadvantaged using OSPF cost and operates as a passive backup.

There are several thousands of users in each area. These users are divided into networks of 4 x 256 IP addresses (4C range), with each network in a separate VLAN. All VLANs are connected to the central VMware cluster for monitoring and testing purposes. This VMware cluster is located in two server rooms in area A and area B. The need for connecting L2 VLANs through the backbone L3 infrastructure

led to a hybrid topology where L2 and L3 traffic is mixed together. Some traffic is routed locally at the nearest router. Other traffic must be switched to the direct router first, before being routed to the remote router.

Spanning Tree Protocol (STP) was necessary to deploy reliable L2 redundancy. The combination of OSPF and STP while functional can also be an ideal option. An OSPF message cannot be delivered to the other side of a physical link between devices because STP is blocking traffic on this physical link. When the status of STP on the physical port is changed from Blocking to Forwarding, OSPF establish a new router adjacency and discovers new routes. These routes are inserted into LSDB and the routing table. Performing these steps is much more complicated than a simple transition to a backup route in OSPF. The convergence time of this combination of protocols is significantly higher than in the case of OSPF itself.

Backbone devices in the student dormitory network use many protocols in addition to the above mentioned protocols (STP, GVRP, OSPF and OSPFv3). These are primarily protocols for the operations of multicast (PIM, IGMP), monitoring (SNMP), assigning IP addresses (DHCP relay, Router Advertisement), access control (ACL) and many others.

This work focuses on the migration of the above-mentioned technology into one virtual chassis assembled from several HP 5800 switches.

## 3 Topology changes

### 3.1 Physical topology

The student dormitory network has four main interconnecting rooms: two of them also serve as server rooms. The original switch technology with STP could not ensure failover for network connection of servers. In order to secure failover for servers, the number of IRF nodes was increased by one in both server rooms, so the IRF virtual chassis consisted of six nodes.

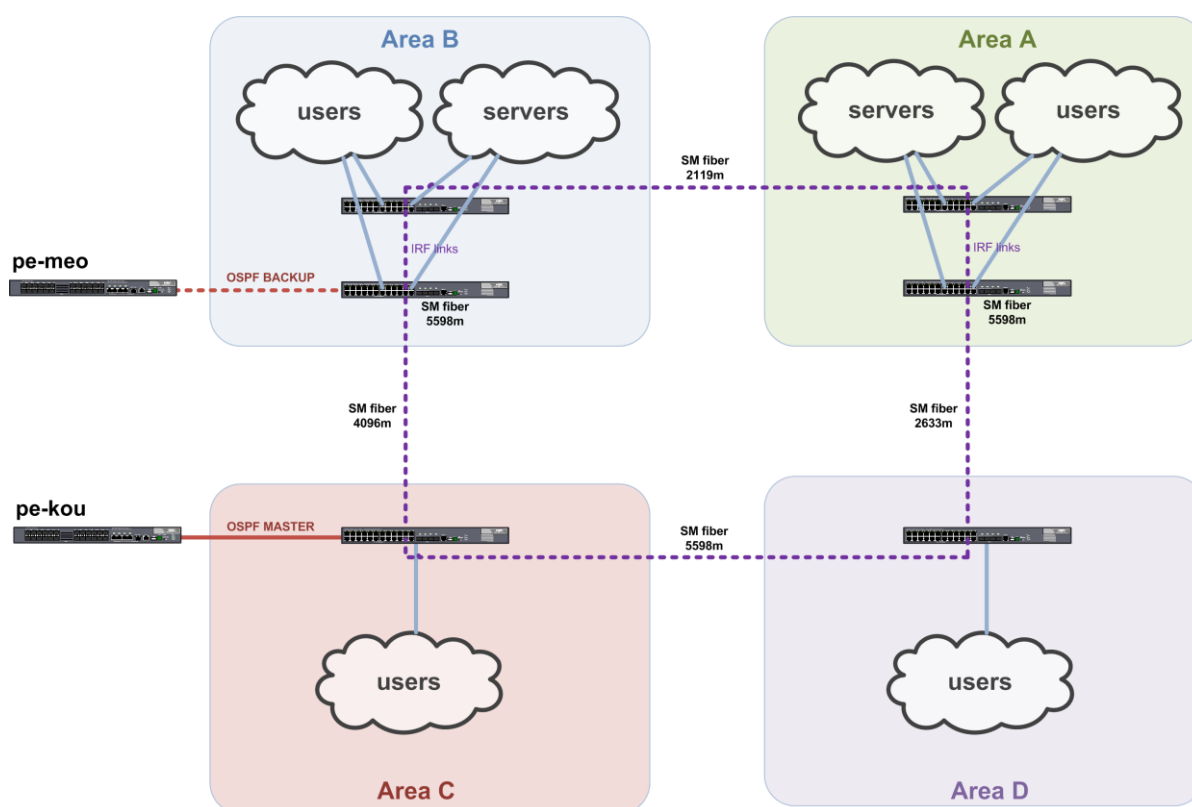


Figure 3.1: Revised network topology



## 3.2 Logical topology

Configuration of most protocols has been significantly simplified because it is no longer necessary to configure and maintain multiple instances of PIM, OSPF, OSPFv3, ACL and DHCP-RELAY. These protocols are set just once on the IRF virtual chassis.

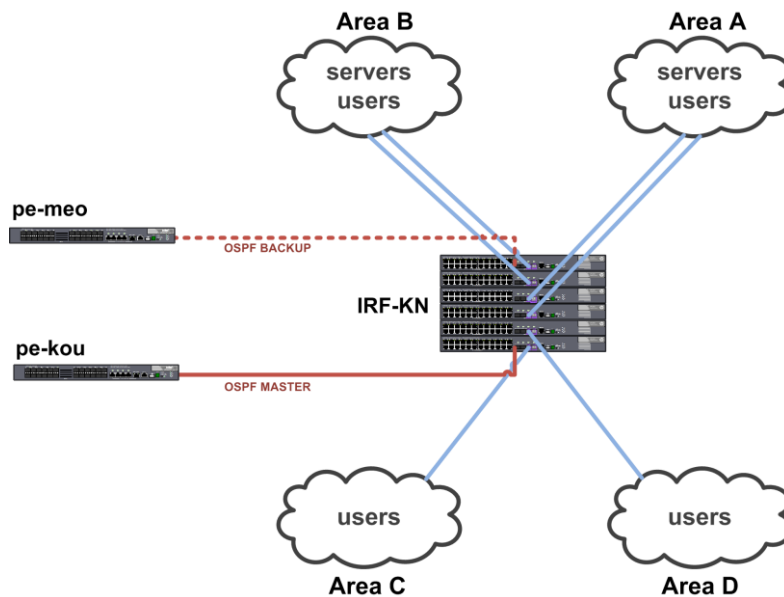


Figure 3.2: Simplified network topology

## 4 IRF configuration

First of all, it is necessary to unify the operating system version on each device that will be connected to the IRF virtual chassis. When the chassis is created, the preparation of the first two nodes is necessary in every case, no matter what size of IRF virtual chassis is eventually created. A serial console to each node is required when configuring the IRF virtual chassis.

### 4.1 IRF from two devices

Node 1:

```
irf member 1 priority 10
```

Node 2:

```
irf member 1 renumber 2
save
quit
reboot
system
```

Node 1:

```
int Ten-GigabitEthernet 1/0/25
shutdown
int Ten-GigabitEthernet 1/0/26
shutdown
```

Node 2:

```
int Ten-GigabitEthernet 2/0/25
shutdown
int Ten-GigabitEthernet 2/0/26
shutdown
```

Node 1:

```
irf-port 1/2
  port group int ten 1/0/26
  quit
int Ten-GigabitEthernet 1/0/26
  undo shutdown
  quit
save
```

Node 2:

```
irf-port 2/1
  port group int ten 2/0/25
  quit
int Ten-GigabitEthernet 2/0/25
  undo shutdown
  quit
save
```

Node 1:

```
irf-port-conf active
```

Node 2:

```
irf-port-conf active
```

A reboot of Node 2 follows. After booting, a basic IRF virtual chassis is prepared. It is appropriate to verify the configuration using the following commands.

```
display irf
display irf configuration
display irf topology
```

## 4.2 IRF from three or more devices

Node 3:

```
irf member 1 renumber 3
save
quit
reboot
system
```

**Node 2:**

```
int Ten-GigabitEthernet 2/0/26
shutdown
irf-port 2/2
port group int ten 2/0/26
int Ten-GigabitEthernet 2/0/26
undo shutdown
quit
save
```

**Node 3:**

```
int Ten-GigabitEthernet 3/0/25
shutdown
irf-port 3/1
port group int ten 3/0/25
int Ten-GigabitEthernet 3/0/25
undo shutdown
quit
save
irf-port-conf active
```

**Node 3:**

```
irf-port-conf active
```

Configuration for other nodes is very similar. The last step for completing the ring topology is creating an IRF connection between node 6 and node 1 (6/0/26 <=> 1/0/25).

## 4.3 ISSU update

In-Service Software Upgrade (ISSU) is a transparent software upgrade capability for IRF virtual chassis.

```
tftp 10.0.0.1 get A5800_5820X-CMW520-R1211P04.bin
display version comp-matrix file flash:/a5800_5820x-cmw520-r1211p04.bin
```

```
Number of Matrices in Table = 1
Matrix for HP A5800-24G Switch
```

```
Running Version:R1211P01
Version Compatibility List:
```

R1211P04 (Compatible)

The ISSU update only works with compatible software versions.

### 4.3.1 Software redistribution

Software must be transmitted to all nodes.

```
copy flash:/a5800_5820x-cmw520-r1211p04.bin slot2#flash:/
copy flash:/a5800_5820x-cmw520-r1211p04.bin slot3#flash:/
copy flash:/a5800_5820x-cmw520-r1211p04.bin slot4#flash:/
copy flash:/a5800_5820x-cmw520-r1211p04.bin slot5#flash:/
copy flash:/a5800_5820x-cmw520-r1211p04.bin slot6#flash:/
```

### 4.3.2 Update procedure

Boot the new software into node 2.

```
issu load file a5800_5820x-cmw520-r1211p04.bin slot 2
```

Verify IRF and boot-loader status.

```
display irf
display device
display boot-loader
```

The newly booted node becomes the master. The original master (node 1) will reboot.

```
issu run switchover slot 2
```

If everything is OK.

```
issu accept slot 2
```

The following command loads the new software in node 1. It involves another reboot.

```
issu commit slot 1
```

The same command is used for other nodes.

```
issu commit slot 3
issu commit slot 4
issu commit slot 5
```

```
issu commit slot 6
```

### 4.3.3 Two node Link Aggregation

A dynamic link aggregation (LACP) for interconnecting a switch or a server to the virtual chassis can be formed with the following commands.

```
interface Bridge-Aggregation 1
  link-aggregation mode dynamic
int ten 1/0/27
  port link-aggregation group 1
int ten 2/0/27
  port link-aggregation group 1
interface Bridge-Aggregation 1
  port link-type trunk
  port trunk permit vlan 10 20 30
```

## 5 Conclusion

The purpose of this document is to describe operating the network virtual chassis in order to use it as a manual to design other virtual chassis.

Today computer networks are affected by many innovations, either in the field of network protocols, security, or in the area of server virtualization. Networks are built with the requirement to maximize the flat network. Virtual chassis technology can greatly help in simplifying the network topology at access and at the aggregation layer and combine these layers on a single logical device and thereby reduce the number of hops to the transit provider. In the end there is no need to run protocols like STP and thanks to the internal distribution of traffic the links between nodes are used more effectively.

At the moment, there are networks where L2 VLANs pass a L3 backbone. A virtual chassis is a good solution for these hybrid topologies. If your network combines L2 and L3, try to consider deploying a virtual chassis. More than two years of practical experience from operating an IRF stack in such an environment showed us that this technology is robust enough to provide services across a wide area in a heavily loaded network.

## References

- [1] Intelligent Resilient Framework  
[h17007.www1.hp.com/docs/reports/irf.pdf](http://h17007.www1.hp.com/docs/reports/irf.pdf)
  
- [2] IRF Configuration Guide  
[http://h20566.www2.hp.com/hpsc/doc/public/display?docId=emr\\_na-c02648772](http://h20566.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c02648772)
  
- [3] NAT Using Source Routing through BGP Gateways,  
Pavel Kislinger, Vladimir Zahorik, September 2013 (CBPD122, the Czech Republic)  
<https://www.terena.org/activities/campus-bp/pdf/gn3-na3-t2-CBPD122.pdf>
  
- [4] Configuration of HP Procurve Devices in a Campus Environment, Tomas Podermanski, Vladimir Zahorik, March 2010 (CBPD111, the Czech Republic)  
<http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-cbpd111.pdf>
  
- [5] Recommended Resilient Campus Network Design, Tomas Podermanski, Vladimir Zahorik, March 2010 (CBPD114, the Czech Republic)  
<http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-cbpd114.pdf>



## Glossary

|                 |                                                                                                |
|-----------------|------------------------------------------------------------------------------------------------|
| <b>BUT</b>      | Brno University of Technology, <a href="https://www.vutbr.cz/en/">https://www.vutbr.cz/en/</a> |
| <b>DHCP</b>     | Dynamic Host Configuration Protocol                                                            |
| <b>DNS</b>      | Domain Name System                                                                             |
| <b>GVRP</b>     | GARP VLAN Registration Protocol                                                                |
| <b>GARP</b>     | Generic Attribute Registration Protocol                                                        |
| <b>IOPS</b>     | Input/Output Operations Per Second                                                             |
| <b>IP</b>       | Internet Protocol                                                                              |
| <b>IRF</b>      | Intelligent Resilient Framework                                                                |
| <b>L2</b>       | Layer 2 - Data link layer of OSI model                                                         |
| <b>L3</b>       | Layer 3 - Network layer of OSI model                                                           |
| <b>OSPF</b>     | Open Shortest Path First                                                                       |
| <b>RSTP</b>     | Rapid Spanning Tree Protocol                                                                   |
| <b>SFP</b>      | Small Form-factor Pluggable Transceiver                                                        |
| <b>SM fiber</b> | Single-mode Optical Fiber                                                                      |
| <b>STP</b>      | Spanning Tree Protocol                                                                         |
| <b>VLAN</b>     | Virtual Local Area Network                                                                     |
| <b>VPN</b>      | Virtual Private Network                                                                        |
| <b>VRRP</b>     | Virtual Router Redundancy Protocol                                                             |

