

# Fusix Networks Service Description

**DISCLAIMER: This document is not binding, unless it is a part of a duly signed Contract.**

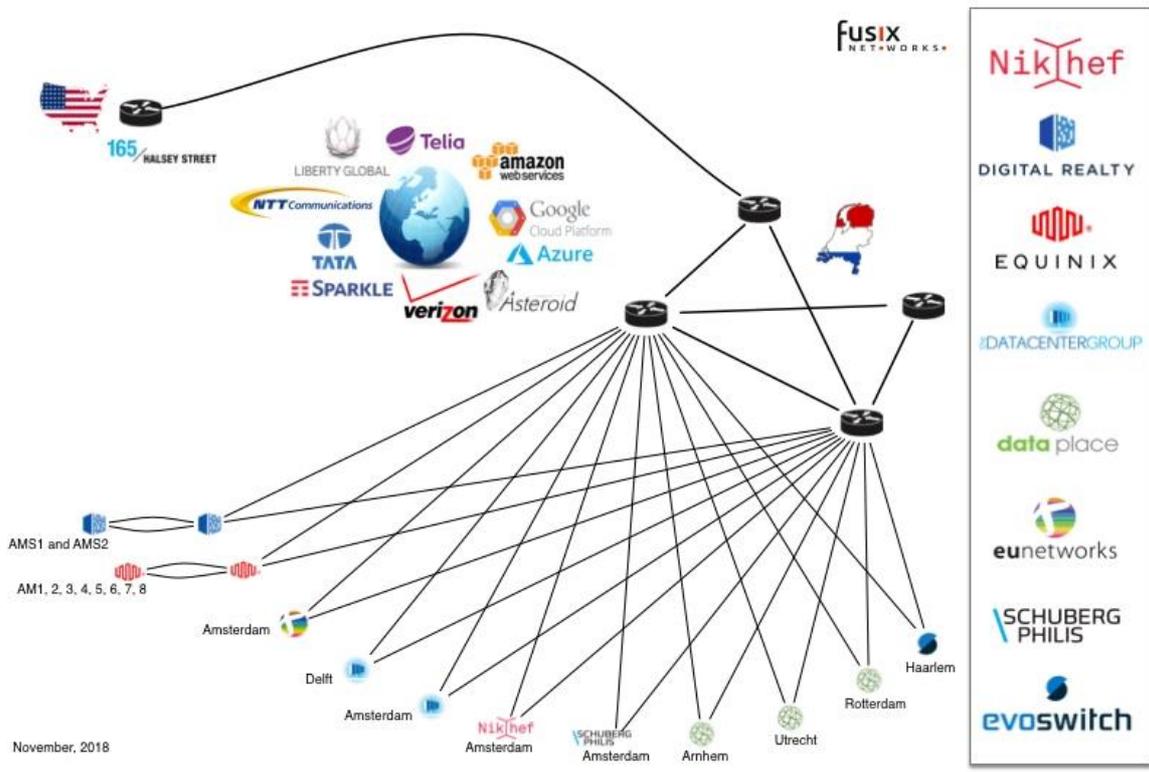
## 1. SERVICE DELIVERY BACKBONE

Fusix Networks B.V. (“Fusix”) is a consulting Internet Service Provider. It helps Clients to design, configure, deploy and manage their own IP networks and connects the networks to the global public Internet. By using Fusix Internet Access services, Clients are in control of maintaining and troubleshooting their network’s connections to the Internet, because the **Team!works on-line portal** provides to them real-time measurements and tools necessary for performing routine network management and troubleshooting tasks. Next to the portal, specialists at the **24/7 Fusix Network Operation Center** stay available to assist and consult Clients on complex questions.

Network Services include **Carrier Services and Internet Access**. They are aimed at hosting, cloud and VoIP providers, ICT and telecommunication companies, office-automation providers and any size of enterprise companies that have business-critical Internet applications. Fusix Clients may use the Network Services for their own benefit or resell them to customers.

Carrier and Internet Access Services are delivered on the Internet Service Provider network of Fusix (“backbone”) that covers The Netherlands (19 on-net data centers in 2018) and the east-coast of the US (1 on-net data center: “165 Halsey Street” in Newark, New Jersey).

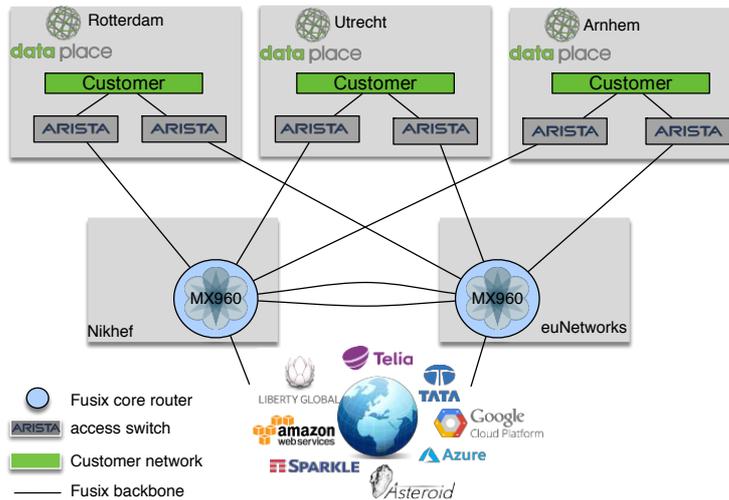
Physical components of the backbone are - among others - Juniper MX960 core-routers, Juniper MX240 and VMX border-routers, Arista edge switches and leased dark-fiber and optical links between the core network and the on-net data centers. Each on-net data center is equipped with a pair of physical switches, each of which is connected to a core router by a fiber-optical connection that follows a different physical path regarding the other path that connects the second switch to another core router. This setup - also known as a “**star-design**” - ensures the lowest risk level of service interruption, because all backbone components and links are deployed redundantly.



Initials Client: \_\_\_\_\_ Initials Fusix: \_\_\_\_\_

The Internet Service Provider (“ISP”) network of Fusix operates on the Internet under the Autonomous System (“AS”) number 57866. It is connected to multiple Tier-1 networks and strategic private peering partners and provides to its users a non-overbooked, high performance access to the global public Internet and dedicated connections to the networks of major cloud providers, such as Amazon, Azure and Google.

Typical delivery of Internet Access and a dedicated connection to a cloud network:



The backbone uses Multiprotocol Label Switching (“MPLS”) for a scalable, protocol-independent data-transport. It allows Fusix to deliver to Clients end-to-end Carrier Services across any type of transport medium, using any protocol. In combination with the star-design of the backbone, another advantage of the MPLS implementation by Fusix is that the uptime of the Internet Access Services does not depend on the uptime of fiber-optical links inside the backbone. Therefore, Fusix delivers to Clients **one of the highest Internet Service Level commitments in the industry, as a part of a standard Internet Service configuration.**

## Network Operation Center (NOC)

Management of the backbone is performed by the Fusix Network Operation Center (“NOC”) in The Netherlands. The management platform has the same name as the Customer portal (“Team!works”). It is deployed redundantly and most of the routine configuration tasks are automated and secured by the in-house developed software, which allows the NOC staff to perform most of the actions fast and without possibility for human errors.

Supervisory activities are also performed by the consolidated diagnostic tools of the Team!works platform and include among others statistics, fault reporting, monitoring of routing behaviors of the Client’s connections and proactive monitoring of the key components: routers, switches and connectivity links.

Continuity, integrity, scalability and security of the backbone are ensured by using **the best practices in the ISP industry** that are selected and adopted by Fusix in line with the standards and requirements of ISO 27000 for Information Security Management Systems and ISO 20000 for Information Technology Service Management. Formal ISO certification is planned to be achieved by the end of 2019.

## 2. NETWORK SERVICES

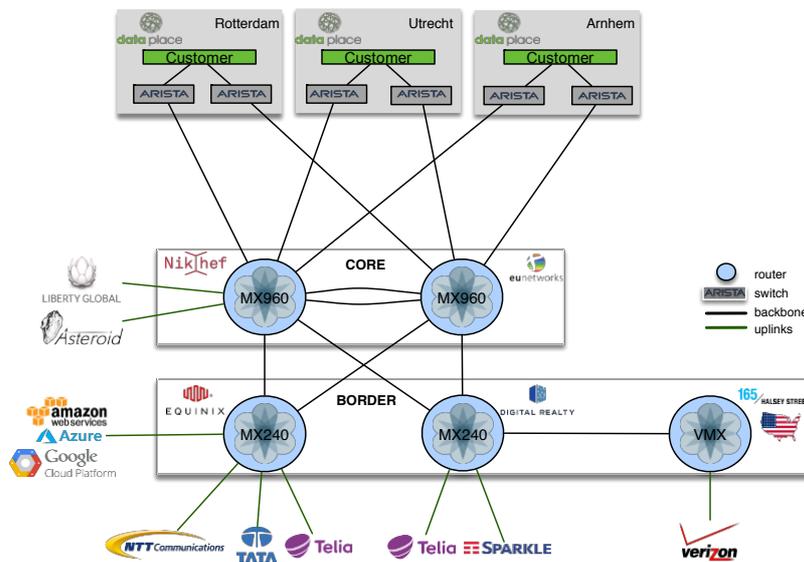
### 2.1 Internet Access services:

- IP transit;
- Direct Internet Access;
- B2B Internet (Internet access at an office address);
- Out of band network management access;
- Direct peering with another ISP network.

Initials Client: \_\_\_\_\_ Initials Fusix: \_\_\_\_\_

Each ISP network on the Internet has its unique Internet resources: an AS number and a block of IP addresses. It announces to all other networks via the Border Gateway Protocol (“BGP”) its own IP address block (prefix) for which it wants to receive IP traffic. All networks listen to these announcements and use them for sending out IP packets. Obviously, not every ISP network on the Internet is directly connected to every other ISP network, thus there are normally 3rd parties’ IP transit networks that are used in the IP packet delivery path.

For each IP packet transmission, the core routers of Fusix will look at the requested destination IP address, find out which ISP network announces it, **run a route security check** using the Resource Public Key Infrastructure (“RPKI”) to verify that the AS that announces the destination IP address is the legitimate owner of the IP address block, calculate the shortest path to that AS by comparing all options that are available from all the Fusix backbone’s uplinks, and send out the IP packet to that path. The uplinks of the Fusix backbone are connected to the border routers, which allows the core routers to make a more knowledgeable and accurate decision on the length of IP packet delivery paths that are offered by the uplinks, instead of choosing an uplink that is directly connected to a core router. In the result, the Fusix backbone **provides a measurable improvement of quality for the Client’s IP routes on the Internet**.



For incoming IP packets, the backbone will receive them from one of the uplinks and hand to the relevant Client’s network. The IP packet delivery path that was used in this case was chosen by the sending network.

### 2.1.1 On-net data centers where Fusix delivers its Internet Services to Clients:

- Digital Realty AMS 1 (Science Park 120, 1098 XG Amsterdam),
- Digital Realty AMS2 (H.J.E. Wenckebachweg 127, NH 1096 AM, Amsterdam)
- dataplace Rotterdam (Van Coulsterweg 6, 2952 CB Alblasterdam),
- dataplace Groenekan (Koningin Wilhelminaweg 471, 3737 BE Groenekan),
- dataplace Arnhem (Tivolilaan 251, 6802 EG Arnhem)
- Equinix AM1/2, Luttenbergweg 4, 1101 EC Amsterdam)
- Equinix AM3 (Science Park 610, 1098 XH Amsterdam)
- Equinix AM4 (Science Park 610, 1098 XH Amsterdam)
- Equinix AM5 (Schepenberweg 42, 1105 AT Amsterdam)
- Equinix AM6 (Amstel Business Park Campus, Duivendrechtsekade 80A, 1096 AH Amsterdam)
- Equinix AM7 (Kuiperberweg 13, 1101AE Amsterdam)
- Equinix AM8 (Gyroscoopweg 2E-F, 1042AM Amsterdam)
- euNetworks (Paul van Vlissingenstraat 16, 1096 BK Amsterdam),
- EvoSwitch (J.W. Lucasweg 35, 2031 BE Haarlem),
- NIKHEF (Science Park 103, 1098 XG Amsterdam),
- The Data Center Group, Amsterdam (Kabelweg 48, 1014 BB Amsterdam),
- The Data Center Group, Delft (Heertjeslaan 1, 2629 JG Delft),
- Schuberg Philis (Boeing Avenue 271, 1119 PD Schiphol-Rijk), and
- 165/Halsey Street (165 Halsey St, Newark, NJ 07102, USA).

**An up to date list is published on the Fusix web-site [www.fusix.nl/ip-transit](http://www.fusix.nl/ip-transit).**

Initials Client: \_\_\_\_\_ Initials Fusix: \_\_\_\_\_

**IPv4 and IPv6.** Fusix AS 57866 supports IPv6 and IPv4 natively and offers full reachability from/to both IPv4 and IPv6 networks.

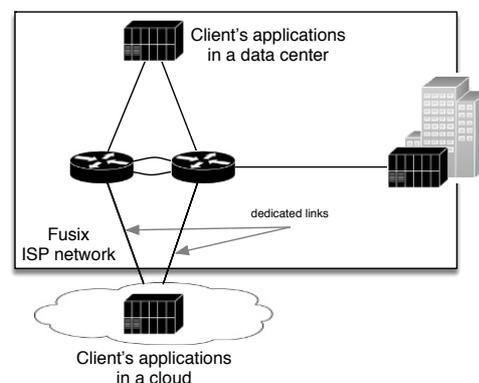
### 2.1.2 Internet Access Service configurations

Internet Access Service can be configured in many different ways, the major differences between them are:

1. If a Client uses Internet resources (IP addresses) that are provided to it by Fusix, the Service is called “**Direct Internet Access**” or “**Out of band network management access**”.
  - a. **Direct Internet Access** connects Internet applications of a Client to the public Internet without the need for the Client to deploy and maintain its own Internet resources. It is an “off the shelf” service with a very short delivery time.
  - b. **Out of band network management access (OOB)** is a low-bandwidth Internet connection that a Client uses to access management interfaces of its IP network devices. OOB is always configured with an IP address of Fusix, which ensures that the management network of the Client is reachable via the Fusix OOB connection in the unfortunate event of outage on the network of the Client.
  
2. If Client has its own ISP network with Internet resources, the Service is called “**IP transit**” or “**Direct peering**”.
  - a. **IP transit** provides to a Client all routes and the Client implements on its network its own policies and preference schedule, according to which in practice the Client’s network will choose a route from all the routes that it is offered.
 

**IP transit with full BGP.** Internet service is configured with a full global Internet routing table, which allows Client to be connected to multiple IP transit providers and choose routes from the options that are offered by all providers. Full BGP is designed to make sure that the IP packets are routed to a Service Provider who offers the best routes. Which routes are “the best” is decided according to preference rules that the Client configures and manages on its side, meaning that the Internet Service Provider(s) do not have a say in the preference criteria of the Client.

**IP transit with default route.** Full BGP service configuration requires that the Client uses powerful routers. If Client has routers capable to process a limited number of routes (partial BGP table), a default route to Fusix will provide the Client with all the Fusix routes, from which the Client can choose a preferred route for sending out IP packets. A link to a second IP transit provider can be added for a diversity of routes for the incoming IP packets. Both providers will deliver incoming IP packets to the Client’s network, while the outgoing packets will be sent (by the default route configuration) to Fusix.
  - b. In a **Direct peering** service configuration, two peering networks send to each other only the routes that they have on their own respective networks, including the routes of the direct clients. This means that each peering network can reach only the IP addresses that belong to the AS number of the other peering network and to the AS(s) of its direct clients.
  
3. **B2B Internet Access** is delivered at a Client’s office location and can be configured as Direct Internet Access or IP transit. A service contract will include a fiber-optical connectivity at the office and the high-quality Fusix Internet Access Service. The physical connectivity is sub-contracted by Fusix from a fiber network operator, such as A-FIBER, KPN, EuroFiber, Ziggo, Tele2, BBNed and provided to a Client together with the Fusix IP service under one contract. The Fusix NOC remains the 1<sup>st</sup> point of contact for both physical and Internet connectivity. Internet Access in a data center, B2B Internet and a dedicated access to a cloud network provider can be all combined to establish a scalable, secure and manageable IP transport between a Client’s office and business applications that the Client hosts in a data center and business applications that are hosted in a cloud network of Amazon, Google or Microsoft Azure. The main advantage of this combination is that the IP transport takes place within the network of one ISP, instead of traveling through the public Internet.



Initials Client: \_\_\_\_\_ Initials Fusix: \_\_\_\_\_

**Pricing model:** a setup fee covers delivery and activation of a fiber connection at the office address, it depends on availability of an on-net or a near-net fiber network. A monthly fee covers maintenance of the fiber and an agreed Internet bandwidth.

## 2.2 Carrier Services:

- CWDM/DWDM wave;
- Virtual Leased Line between 2 locations (point to point);
- Virtual Leased Line between >2 locations (point to multipoint);
- Redundant Virtual Leased Line.

Fusix leases a dark fiber infrastructure between its core routers and the most of its on-net data centers. On this dark fiber infrastructure, it built and maintains fiber optic transmission: wavelength-division multiplexing (**WDM**). WDM systems are divided into 2 different wavelength patterns: coarse (**CWDM wave**) and dense (**DWDM wave**). Both are based on the same concept of using multiple wavelengths of light on a single fiber, but differ in technical specifications of the wavelengths, number of channels, and the ability to amplify the signals. CWDM does not have optical amplification, which results in limiting the distance of the CWDM connections to several tens of kilometres.

WDM is point to point connection over a physical fiber path, therefore it cannot be redundant. If critical services rely on a wave, it is recommended to order 2 waves, each of which will use a separate fiber path. In this case, one of the waves will remain available, in the unfortunate event of a problem with one of the fiber paths.

Normally, connecting a WDM wave requires from Client to use a WDM transceiver (with an agreed colour) and to order a separate data center cross connect to Fusix; however – as an additional service – Fusix can deliver a WDM wave on a standard multi-mode or a single mode (LR/SR) transceiver to reduce the cost of service implementation for the Client. The Client can use a less expensive transceiver on its side and receive the service as a VLAN over an existing cross connect. **One WDM wave has the capacity of carrying 10Gbit of IP traffic.**

**Virtual Leased Line (“VLL”)** is a data transmission service delivered on the Ethernet interface. It is a virtual layer 2 connection between two (or more) network nodes, also often referred to as “VLAN”. It is useful, if a Client has network nodes at multiple data centers and wishes to consolidate them into one network with the same security, reliability and manageability requirements of a private network. Using VLL, the Client avoids a cost of building and maintaining a fiber-optical connectivity between the nodes, while the main goal of a consolidated secure network is achieved.

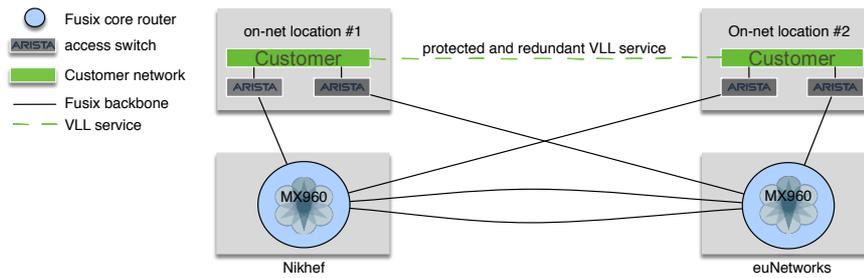
**Fusix offers fixed or dynamic VLL capacity, with Q-in-Q and jumbo-frame capabilities (Maximum Transfer Unit at least 9000 bytes).**

A VLL can connect 2 data center locations (“point-to-point”) or one data center to multiple data centers (“point-to-multipoint”). Each use case has a best practice configuration, however different combinations are possible depending on specifics of the Client’s network design.

For a point-to-point VLL, the standard setup is *Edge switch – core router – Edge switch*. A tailored setup would account for a future plan to convert a point-to-point VLL to a point-to-multipoint VLL, in which case the VLL would be delivered from start as *Edge switch – core router #1 – core router #2 – Edge switch*. This setup has a VLL Service **protection** on the lag between the core routers, meaning that if one link between the routers is down, there is still no VLL Service interruption.

Further, VLL Service can have **redundancy**, meaning that there will be 2 active VLLs, each of which uses a separate (redundant) fiber optical path and network devices. This configuration dramatically reduces the risk of Service availability impact in case of planned maintenance or an unfortunate failure of any component of the Fusix backbone. In the normal scenario, both VLLs are configured to behave as a single link with a double data-throughput. The picture below shows the fiber optical links (black lines) that carry a redundant VLL Service (dotted green line) between 2 data centers:

Initials Client: \_\_\_\_\_ Initials Fusix: \_\_\_\_\_



### 2.3 Typical commercial propositions

Prices in this document are public. Fusix encourages its potential Clients to request a tailored Service Proposal by contacting [office@fusix.nl](mailto:office@fusix.nl) or T: +31 (0) 85 401 4441.

#### Fixed-fee Internet Access with redundant service-delivery paths:

- Aggregated billing of an agreed Internet bandwidth commitment. Clients are allowed to use the bandwidth on all their physical connections with Fusix combined, even if the connections are in different on-net data centers;
- Service uptime guarantee 99.999% per data center;
- Redundant service delivery paths: Internet Service is delivered on 2 physically redundant ‘active-active’ paths, which reduces the impact of planned maintenance activities and the risk of Service impact in an unfortunate event of failure of any of the Fusix backbone components;
- Resource Public Key Infrastructure (routing security mechanism);
- Service configuration as DIA or IP transit. For IP transit: full BGP or a default route configuration;
- Reachability to/from IPv4 and IPv6 networks;
- IPv4 and IPv6 addresses for connecting to the Fusix backbone;
- Burst-bandwidth measurement according to the 95-percentile model: first, 5% of the highest bandwidth usage peaks is disregarded, then the next available value is used for billing;
- Access to Fusix Team!works: 24/7 password-protected Service monitoring and IP-networking tools.

Internet bandwidth:	100 Mbps	250 Mbps	500 Mbps	1 Gbps
Active ports facing the Client’s network:	2 x 1 Gbit	2 x 1 Gbit	2 x 1 Gbit	2 x 10 Gbit
Setup fee:	€ 250	€ 200	€ 150	n/a
Monthly:	€ 265	€ 335	€ 625	€ 1 050

#### Managed Internet Access Package (MIAP)

MIAP package is a combination of (i) quality features of Internet Access with redundant service-delivery paths, and (ii) **24/7 response by the professional Fusix NOC to management and troubleshooting requests concerned with the Client’s IP network.**

	MIAP 500 Mbps	MIAP 1 Gbps
<b>BASIC availability SLA:</b> response by a qualified network engineer within 4 hours 24/7 to urgent requests; and within 3 working days during Business Hours to non-urgent requests	✓	premium
<b>PREMIUM availability SLA:</b> response by a qualified network engineer within 2 hours 24/7 to urgent requests; and within 2 working days during Business Hours to non-urgent requests	n/a	✓
<b>BASIC DDoS mitigation:</b> assistance with identifying the target of a DDoS attack, then blackholing of the target. Blackholing drops all IP traffic, which removes congestion and allows to keep other network services live during the attack. However, the target IP address remains isolated from the Internet.	✓	✓
<b>ADVANCED DDoS mitigation:</b> Fusix NOC will provide best-effort <u>filtering</u> of malicious traffic. Successful filtering allows all network services, including the attack-target to stay live, because only malicious traffic is dropped.	n/a	✓

Initials Client: \_\_\_\_\_ Initials Fusix: \_\_\_\_\_

Monitoring of the Client's IP network performance: statistics, history and diagnostics, excluding a wake-up alert functionality.	✓	✓
NOC consultancy hours for problems outside Fusix Internet Service (only non-urgent requests) included per month	1	3
Hourly rate for non-urgent assistance	€ 80	€ 80
Hourly rate for urgent assistance and assistance outside Business Hours	€ 135	€ 135
<b>Monthly:</b>	<b>€ 850</b>	<b>€ 1.365</b>

Clients may combine any of the NOC services in Section 3.2 (“Client’s IP network management”) with any Internet Access Service, to create their own customized MIAP packages.

**Flat fee Internet Access with a single (non-redundant) service-delivery path:**

- Internet bandwidth as much as allowed by the capacity of a port: up to 1 Gbit or up to 10 Gbit,
- Service uptime guarantee 99.95% per port,
- Service SLA for delivery, performance, availability and time-to-restore. *Details are provided in the “Fusix Network Services SLA” document,*
- Service configuration as DIA or IP transit. For IP transit: full BGP or a default route configuration,
- Full reachability to/from IPv4 and IPv6 networks,
- IPv4 addresses required for connecting to the Fusix backbone,
- Access to Fusix Team!works: 24/7 password-protected Service monitoring and IP-networking tools.

Port:	1 Gbit	10 Gbit
Setup fee:	€ 150	€ 150
Monthly:	€ 795	€ 6.035

### 3. NETWORK CONSULTANCY

Network consultancy services are offered only in combination with Fusix Internet or Carrier Services. Consultancy includes: (i) Projects, (ii) Management of IP networks of the Clients, and (iii) regular release of new IP networking tools by adding them to the Team!works portal, which results in putting the Clients in control of management and troubleshooting of their connections to the Internet.

#### 3.1 Consultancy projects

Consultancy project contains professional research of business and technical requirements, network design, equipment options and a quote, assistance with receiving IP addresses from the Regional Internet Registry “RIPE NCC”, IP address plan, network configuration, deployment plan and installation. It can be used for building a new network or for an existing network’s migration or upgrade.

Regarding network configuration in particular, on the global Internet, countless networks talk to each other by using the BGP protocol. It allows each network to have its own routing policies with multiple criteria, such as the shortest path, price, latency etc. BGP policies define how a network responds to the users of the services that the network offers on the Internet. Fusix consultants are BGP professionals, widely recognized in the Internet Service Provider community. They make sure that the requirements of the Client’s business are translated into the BGP language correctly and with nuances.

**Best-seller projects:**

**New IP network design and implementation, fixed one-off fee € 2.000**

- IP network design:
  - ✓ address technical, business and budget requirements and goals of the Client;
  - ✓ propose matching best practices for the network availability, integrity, scalability and security;
  - ✓ IP address plan,
  - ✓ network hardware and internal connectivity proposal;
  - ✓ (optional) quote for leasing network components;

Initials Client: \_\_\_\_\_ Initials Fusix: \_\_\_\_\_

- ✓ (if matches the requirements) registration of the Client's business entity with the "RIPE NCC" Regional Internet Registry, receiving IPv4 and IPv6 blocks and an AS number, filing of BGP policies

- half-day detailed technical session:
  - ✓ presentation of a draft network design;
  - ✓ Q&A, joint brainstorming;
  - ✓ follow up fine-tuning and adjustments of the design;

- Design-implementation plan;

- Configuration of the core network hardware (routers and switches);

- 1 x hands-on installation of the Client's servers, firewalls, routers and switches on the Client's site;

- Network documentation.

### **IP network migration, fixed one-off fee € 3.900**

- For the target network setup: a full scope of the "New IP network" project, including design, ½ day technical Q&A, core network configuration and a matching hardware/connectivity proposal;

- Migration plan:
  - ✓ address the Client's requirements, such as time-schedule, on-going contracts, deadlines etc;
  - ✓ review of the existing network;
  - ✓ assessment of a technical impact on the existing users;
  - ✓ a high-level plan for deployment of new components, re-establishing of re-usable components on the target network and decommissioning of obsolete components;

- half-day detailed technical session about a draft migration plan:
  - ✓ presentation of the design;
  - ✓ Q&A, joint brainstorming;
  - ✓ follow up adjustments;

- Migration management:
  - ✓ detailed implementation plan;
  - ✓ close coordination of activities within each implementation phase;
  - ✓ dedicated Fusix PoC for project management;
  - ✓ dedicated Fusix technical PoC;
  - ✓ dedicated Fusix hands-on engineer;

- Execute the agreed plan.
  - ✓ Without additional cost: 3 network migration windows of 12 work hours (in total) provided either within or outside Business Hours, to reduce impact of the migration activities on the existing users;

- Network documentation.

### **Second consultant opinion, fixed one-off fee € 3.500**

Analysis and evaluation of an existing network design or a network migration plan, including advice on improvements, discussion of (dis-)advantages, suggestion of additional ways to minimize business impact.

If required, an alternative network design or implementation plan will be suggested by Fusix.

Client is the owner of all the materials that Fusix produced for the purpose of the analysis and evaluation. The Client will also decide in its own discretion, which company will execute the final project-plan.

### **Data center layout, fixed one-off fee € 350**

Initials Client: \_\_\_\_\_ Initials Fusix: \_\_\_\_\_

Layout for one or more data center racks according to the Client’s requirements and the best practice of intelligent network-installations in a data center environment. Complete documentation, including rack layout and connectivity diagrams are included.

Deployment can be performed by a professional Fusix field engineer according to the terms of “Smart hands and eyes” service.

### “Smart hands and eyes” at a data center

The service is provided in any data center in the Netherlands, separately from the Fusix Network Services.

For a one-time project, a time-schedule and a work-scope must be agreed at least 3 Business Days in advance to ensure availability of a professional data center engineer with relevant qualification level.

Clients who require maintenance of their data center infrastructure on a recurring basis are offered a **Service Level for the on-site availability of a professional data center engineer**. The Service Level is: within 4 hours on-site presence for an urgent task; and within 2 Business Days within Business Hours work for non-urgent tasks.

In addition to tasks that are delivered on-site, non-urgent Smart hands and eyes tasks may include activities in the Fusix office, such as for example:

- ✓ receiving hardware shipments,
- ✓ intelligent unpacking with a video recording to control any damage on delivery,
- ✓ hardware preparation for installation in a data center: in the Fusix office Lab, a qualified network engineer will install a requested OS, upgrade a vendor software/firmware to the latest version (if the hardware has a valid vendor-support contract) and configure the hardware for a remote access by the Client’s IT team.

#### Smart hands and eyes service prices:

On-site presence SLA (mandatory for recurring requests)	€ 750 / month
Non-urgent tasks delivered within Business Hours	€ 65 / hour
Non-urgent tasks delivered outside Business Hours	€ 135 / hour
Urgent tasks	€ 135 / hour
Travel fee to any data center in The Netherlands	€ 50 / travel by one person

## 3.2 Management of the Client’s IP network

Clients who receive Fusix Internet or Carrier service(s), may also use knowledge and expertise of the Fusix NOC to **manage and troubleshoot the Client’s network and its connections to the Internet**. The scope of IP management services includes, among others, network monitoring, configuration, backups, tuning of BGP policies, DDoS mitigation, adding a 3<sup>rd</sup> party Internet peer, network hardware recommendation and sales, and troubleshooting of problems/configurations on the side of the Client’s network.

**The Service is offered as: (i) stand-by availability, or (ii) full 24/7 management.**

1. **24/7 guaranteed stand-by availability of a Fusix networking professional to assist with management and troubleshooting of the Client’s IP network.** It provides Clients with a 2<sup>nd</sup> line IP networking support by a Fusix consultant who knows the setup of the Clients and can assist within a guaranteed time limit with advanced troubleshooting tasks to pinpoint a problem.

<b>BASIC:</b> response by a qualified NOC engineer within 4 hours 24/7 to urgent requests; within 3 working days during Business Hours to non-urgent requests	€ 300/month
<b>PREMIUM:</b> response by a qualified NOC engineer within 2 hours 24/7 to urgent requests; within 2 working days during Business Hours to non-urgent requests	€ 350/month

Networking assistance, if provided, is billed at 80 euro for Business Hours and 135 euro for urgent troubleshooting requests and for outside Business Hours.

Initials Client: \_\_\_\_\_ Initials Fusix: \_\_\_\_\_

2. 24/7 IP network management means that **the Fusix NOC takes the responsibility for the well-being of the Client's core IP infrastructure (routers and switches) and their connections to the Internet.** The NOC will monitor the Client's network 24/7 and receive "wake-up" alerts, in case any of the network's performance criteria drops below an agreed level, and act as soon as possible but no later than within 2 hours to troubleshoot a problem and restore the performance level.

24/7 IP network management service has a setup fee that covers a network documentation project. The purpose of the project is to produce a clear technical agreement about measurable criteria of the network performance, document which components will be monitored, which 3<sup>rd</sup> party suppliers play a role in the well-being of the Client's network and how the Fusix NOC can reach out to them on behalf of the Client. **The setup fee is 3.500 euro.**

Based on the management tasks that are agreed by the end of the network documentation project, Fusix will make a final commercial proposal for the 24/7 IP network management service. To provide an example of how commercial terms are put together, an IP network with /22 IP address prefix, 2 Internet providers (one of which is Fusix) and multiple data center locations, requires 5 – 7 work hours per month to be spent on routine management. **A monthly fee would be around 1.225 euro, including 7 hours of network management/troubleshooting by an experienced IP network engineer any time 24/7 when required, pro-active monitoring and a PREMIUM response to urgent alerts.** To spread the work hours across a longer period of time and avoid losing unused hours by the end of a month, Clients normally pay the fee on a quarterly basis.

**Routine management tasks are:**

- ✓ 24/7 pro-active monitoring,
- ✓ backup of network configurations,
- ✓ network monitoring statistics,
- ✓ configuration changes on the Client's core routers and switches,
- ✓ BGP policy management,
- ✓ administration and troubleshooting of core routers and switches, provided that they have valid vendor-support contracts.

### 3.3 Team!works

Team!works on-line portal is a way to share the experience of Fusix professionals with management of large networks. It provides real-time information and self-service tools for routine management and troubleshooting of the Client's connections to the Fusix backbone. The on-line tools available to Clients are fully integrated with the internal Fusix IP network management platform, which enables 24/7 immediate access to information relevant for monitoring Client's connections (via Fusix) to the Internet and pro-active response to security threats, such as a DDoS attack.

**The portal provides at the moment (November 2018):**

- Graphs with IP bandwidth usage;
- Netflow analysis;
- Status of the service-delivery ports on the Fusix side;
- Status of BGP sessions;
- Automated or manual processing of the Client's IP-prefix changes for Clients with a BGP network;
- Reverse DNS;
- DDoS mitigation tools:
  - global blackholing,
  - blackholing outside Netherlands (payable service subscription is required),
  - drop ICMP traffic,
  - drop UDP traffic.

***Fusix continuously releases new network tools, alerts and monitoring measurements via the Team!works portal.***