



Edge Device for a Campus Network

Best Practice Document

Produced by CSC/FUNET led working group on AccessFUNet

Author: Jani Myyry

Contributors:

Kaisa Haapala/CSC- IT Center for Science

Janne Oksanen CSC- IT Center for Science

Janne Niemi CSC- IT Center for Science

13.05.2011

© TERENA 2010. All rights reserved.

Document No: GN3-NA3-T4-Edge-Device
Version / date: 13.05.2011
Original language: Finnish
Original title: "Kampusverkon reunalaitte"
Original version / date: 1.0 of 13.05.2011
Contact: jani.myyry (at) csc.fi

CSC/Funet bears responsibility for the content of this document. The work has been carried out by a CSC/Funet led working group on AccessFunet as part of a joint-venture project within the HE sector in Finland.

This translated version is based on the Finnish counterpart approved by the CSC/Funet annual general meeting on 13 May 2011 after an open consultation period of two weeks.

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 Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 238875, relating to the project 'Multi-Gigabit European Research and Education Network and Associated Services (GN3)'.



Table of Contents

1. Introduction.....	4
2. Edge Device	4
2.1. Features	5
2.2. Hardware Architecture and Protections	6
2.3. Performance	7
3. Edge Device Types	8
3.1. Router and Routing Switch	8
3.2. Firewall	8
4. Topology Examples	9
5. Router or Routing Switch as the Edge Device.....	11
5.1. Pros	11
5.2. Cons	11
6. Firewall as the Edge Device	12
6.1. Pros	12
6.2. Cons	12
7. Edge Device Features	13
7.1. Main Funet Connection	13
7.2. Redundant Funet Connection.....	14
7.4. Light Paths.....	15
7.5. Other Features	15
7.5.1. Fault Tolerance, Duplexed Components	15
7.5.2. Maintenance and Management Features	15
7.5.3. Device Support and Software	16
7.5.4. Connection of the Edge Devices to the Switch Infrastructure (Layer 2).....	16
7.5.5. Protections in the Switch Infrastructure (Layer 2)	16

1. Introduction

This document is a compilation of issues that should be taken into consideration when purchasing an edge device for a campus network and connecting it to the network, and different topology alternatives with their pros and cons.

The purpose of this document is to assist Funet members in their edge device purchasing decisions by providing guidelines on the features the edge device should preferably have. This document does not comment on the manufacturer or model of the edge device.

2. Edge Device

Each organisation has an active network device through which data communications connections are handled from the organisation's network to the outside. In this document, this active network device is referred to as a 'campus network **edge device**'. Different types of devices can act as an edge device; most typical edge devices are routers, routing switches and firewalls.

Edge devices have a couple of basic tasks that are required to enable functional data communications connections:

1. **IP packet forwarding based on routing information** (mandatory)
2. **Traffic filtering, access control lists** (mandatory)
 - protection of the infrastructure (e.g. prevention of address spoofing)
 - protection of the edge device itself (access control, limiting the waste of resources)

- filtering of undesired traffic, or “firewalling” (additional feature)
3. **Changing routing information with routing protocols** (mandatory with redundant connections)
 4. **Traffic classification and prioritisation** (useful)

2.1. Features

Depending on the vendor, network devices support a varying number of features; for example, some devices support dynamic routing protocols, while others do not. Feature-wise, a device may be a very suitable edge device for, say, a connection with no redundancy, but is not useful for redundant connections due to a lack of support for dynamic routing protocols.

The basic requirement for a Funet edge device is support for static unicast routing, enabling the edge device to be used with a non-redundant Funet connection. A redundant Funet connection requires the edge device to support dynamic routing protocols, in particular BGP [RFC4271]. In the case of duplexed edge devices, support for an internal routing protocol such as OSPF [RFC2328] [RFC5340] or IS-IS [RFC5308] is also useful, as the devices can exchange routing information with each other. Multicast also requires support for static or BGP multicast routing [RFC4760], PIM-SM [RFC4601] and possibly PIM-SSM support [RFC4607], and the corresponding protocols towards the Local Area Network (IGMPv2 or IGMPv3 and MLDv2) [RFC5186].

The edge device should also be capable of at least basic filtering in order to block spoofed addresses and misconfigurations. In particular, traffic intended for the Local Area Network should not be let leak out, or accepting traffic from the outside with source addresses in the organisation’s own address space. For more information on filtering, please refer to the BCP 38 and BCP 84 recommendations [RFC2827][RFC3704]. It should also be possible to control administration access to the edge device at least based on the source address.

The edge device should also preferably support traffic classification and prioritisation (QoS). Traffic classification and prioritisation can be used to protect critical traffic during overload or attack situations [RFC4732]. In blocking attacks, features allowing the blocking of traffic from the attackers’ addresses or traffic to the service under attack in the edge device, Funet core network or even NORDUnet are also useful [RFC5635] [RFC5575].

For a more detailed breakdown of edge device features, see Chapter 7. ‘Edge Device Features.

2.2. Hardware Architecture and Protections

The hardware architecture of edge devices can vary depending on the hardware type, performance and purpose of use. Typically, three different operational planes can be noticed from edge devices (Figure 1): IP packet traffic forwarding plane, IP packet traffic control plane, and the network device management plane. However, the planes are not separate in all edge devices; the same hardware resources such as the CPU can handle several planes.

The IP packet traffic forwarding plane handles the most important task: traffic forwarding, filtering, classification and prioritisation based on pre-defined rules. The control plane controls the forwarding plane by defining a routing information base (RIB) and, based on the routing information base, maintaining forwarding information base (FIB) rules, according to which the forwarding plane operates. The control plane typically handles things like routing protocols. The management plane enables monitoring and maintaining the edge device by providing interfaces to both maintenance personnel and monitoring systems.

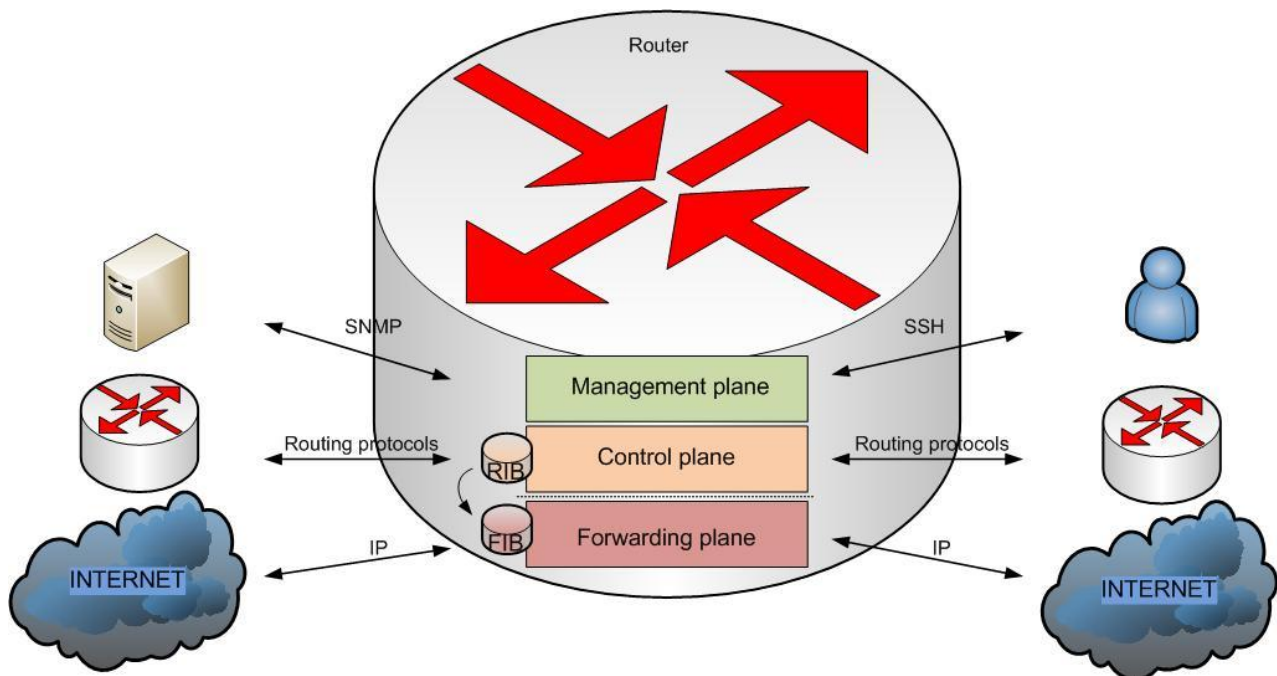


Figure 1. Operational planes of an edge device

In modern edge devices, the operational planes are separated and protected from each other, allowing any disruptions to be limited and the hardware performance optimised according to its task. On the IP packet forwarding plane, chips optimised for the task are typically used. This means that the hardware load will not significantly affect the operation of the edge device even when the traffic profile is not optimal, as is often the case during, for example, Distributed Denial-of-Service attacks.

By separating the forwarding plane from the other planes [RFC3654], the control and management planes can be protected [CPP] so that they accept only the required traffic, such as routing protocol sessions and administration connections from specified source IP addresses. It should be noted that all devices do not support the separation and protection, and there may not be optimised hardware on the forwarding plane. These devices typically have a significantly greater risk of operational disruptions.

2.3. Performance

When the performance of an edge device is evaluated, the device’s performance during IP packet handling should also be taken into consideration in addition to the connection speeds (e.g. 1 Gbps or 10 Gbps). Packet traffic performance is commonly measured by packets forwarded per second (pps).

In order to ensure disruption-free operation, the edge device should be able to handle packet forwarding at the speed determined by the connections under any traffic profile. For example, 1 Gbps traffic speed with minimum packet size (taking the minimum Ethernet frame and the delay between frames into consideration) means around 1.5 Mpps. Correspondingly, a traffic speed of 10 Gbps means around 15 Mpps (Table 1).

Various traffic filtering may also affect performance, possibly reducing the nominal speed, in particular in hardware with no optimised chips on the forwarding plane. Similarly, performance may differ with IPv6 due to the implementation of the optimised chips. In the worst case, IPv6 has been retrofitted in the hardware without hardware-supported optimised packet forwarding, resulting in marginal IPv6 performance compared to IPv4 performance.

Speed / Size of Ethernet frame	64 bytes	64/1518 bytes (50%/50%)	1518 bytes	9018 bytes
100 Mbps	149 kpps	15.4 kpps	8.13 kpps	1.39 kpps
1 Gbps	1488 kpps	154 kpps	81.3 kpps	13.9 kpps
10 Gbps	14881 kpps	1541 kpps	813 kpps	139 kpps
100 Gbps	148810 kpps	15413 kpps	8127 kpps	1386 kpps

Table 1: The effect of Ethernet frame sizes to packet forwarding performance requirements

3. Edge Device Types

3.1. Router and Routing Switch

Modern routers are designed to forward, filter and classify IP packets at line rate regardless of the traffic profile. This property is achieved by utilising chips designed for the purpose for packet forwarding, as hardware and CPUs designed for normal server use are unable to handle the number of packets required by high line rates.

Similarly, routers typically have a control plane that is separated from the forwarding plane. This means that the traffic amounts will not affect the other operations of the hardware such as the routing protocols and the device monitoring and administration. Routing switches are typically similar to routers with the difference of slightly more limited feature set and the emphasis on the switch functionality in the technical solutions.

3.2. Firewall

Firewall is a device with the primary task of filtering traffic, typically using a state based filter, and possibly taking other traffic contents into consideration in addition to protocol, address and port information. Firewalls can also act as secondary routing equipment, allowing firewalls to be used as edge devices.

Firewalls differ from routers generally by performance and operation during network disruptions: firewalls are seldom able to handle traffic at line rate regardless of the traffic profile, because firewalls have limited resources, such as the connection state table size which can be overloaded. Additionally, in firewalls the packet traffic forwarding plane is not typically separated from the control plane, which means that disruptions on the forwarding plane affect the control plane and vice versa.

4. Topology Examples

For the Funet edge device, two different topology alternatives are presented, one of which is implemented with routers or routing switches, and the other with firewalls. The models use some basic components that are the same:

- The Funet network, the core network to which the organisation connects to with the edge device
- DMZ, networks visible to the Internet, typically for servers and requiring only stateless filtering
- R&E network, networks intended for research and education use, offering faster connections or freer use
- Campus, regular workstation networks or server networks only intended for internal use, possible stateful filtering

In the first alternative (Figure 2), the edge device is either a router or a routing switch, to which the Funet network is connected. The DMZ and R&E networks are also connected to the routers, as are the regular campus networks, possible protected with firewalls. In this solution, the possible protection of the DMZ and R&E networks is handled using stateless access lists in the edge routers.

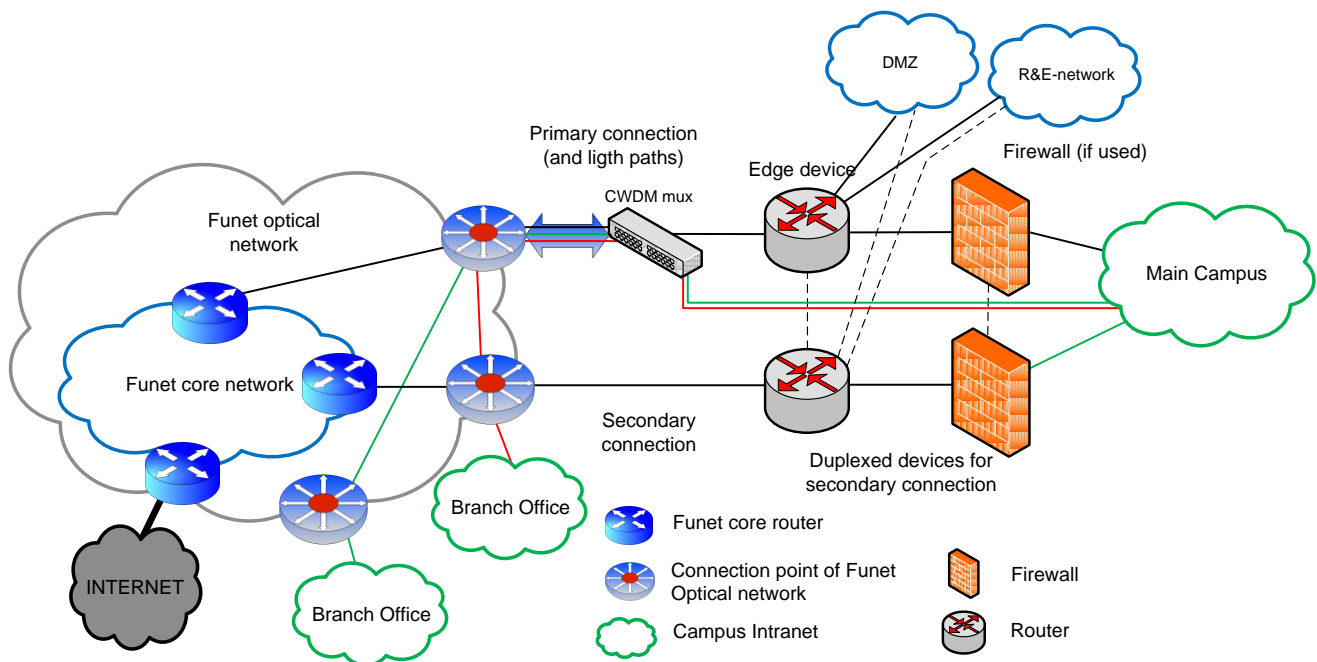


Figure 2: Router as the edge device

In the second alternative (Figure 3), the edge devices are routing firewalls. As in the previous example, the DMZ, R&E and campus networks are connected to these firewalls. The traffic to all networks and services is filtered and forwarded by these firewalls.

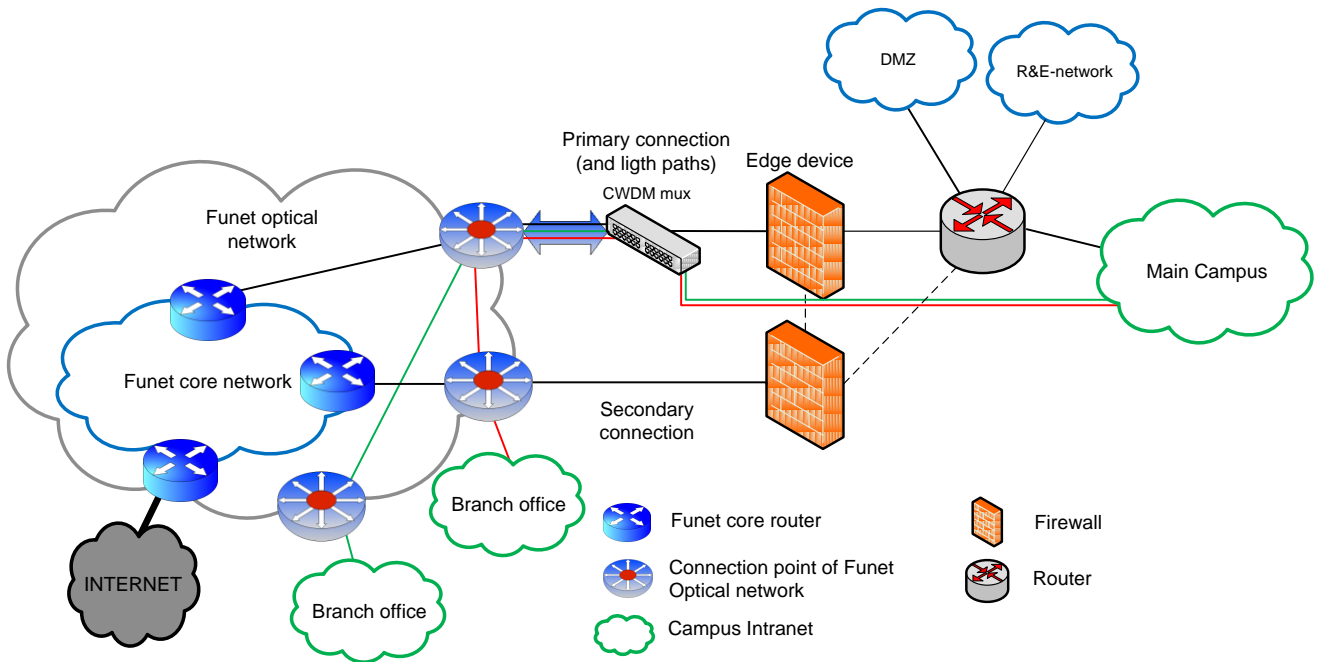


Figure 3: Firewall as the edge device

Connections from branch offices are connected to the main campus network, forming a part of the organisations intranet, so they will not be separately discussed in this document. In the Figures 2 and 3, the branch offices are included in order to illustrate their connection to the topology.

Both models have their pros and cons. The following chapter aims to describe the differences of the models in more details so that it would be easier to select one or the other based on the features, or start looking for a different solution.

5. Router or Routing Switch as the Edge Device

5.1. Pros

- Performance typically matches the connection speeds, including the packet handling performance
- 10GE widely available, scalability to 40GE/100GE available
- Typically wide selection of features
- Routing protocols
- Multicast
- Stateless filtering (access control lists) with no performance hit
- Duplexing and redundant connections easy to implement due to statelessness
- Fewer technical limitations considering R&E networks (e.g. performance, extensive feature support, prior support for new features)
- Quite typically the packet traffic forwarding plane and control/management planes are separated and protected from each other
- Denial-of-service attacks will not affect the operations of the entire organisation. If the bandwidth of the Funet connection is sufficient, the entire organisation will not drop out of the Internet
- The operations of the target of the attack may be disrupted

5.2. Cons

- Offers only stateless filtering (access control lists)
- Separate need for a firewall, if stateful filtering is required (policies)

6. Firewall as the Edge Device

6.1. Pros

- One device can handle the tasks of the edge device and stateful firewall
- Integrated graphical management systems available
- IDS/IPS functionality available

6.2. Cons

- Performance is typically the connection speed "in good conditions"; in particular, packet handling ability is limited
- 1GE available, 10GE challenging or very expensive, 40GE/100GE not available
- Feature set varies by manufacturer
- Support for routing protocols is rare
- IPv6 support non-existent or lacking
- Multicast support non-existent or lacking
- Amount of filtering affects performance, in particular in firewalls with no optimised chips
- duplexing and redundant connections require state synchronisation between the firewalls
- May place limits on R&E networks; in particular the performance and lack of support for modern technologies
- Only a few firewalls separate the packet traffic forwarding plane from the control and management planes
- Denial-of-service attacks may affect the operations of the entire organisation, if the packet forwarding capacity or number of connections are exceeded
- Attack is stopped at the edge device, the target may operate but outside connections not

For a redundant connection, the edge device may be duplexed, or the fault tolerance can be implemented by duplexing the key components inside a modular edge device.

It may be sensible to acquire a redundant connection even if the edge device is not duplexed, in particular when the distance between Funet's fibre network connection point and the closest Funet router is long. The probability of a cut fibre is proportional to the length of the fibre connection, and repairing a cut fibre may take days at worst. Replacing or repairing an edge device is often done during the same day. The response time is affected by the device's service agreements and the available personnel and spare part resources.

7. Edge Device Features

Connecting to the Funet network means that there are some mandatory requirements for the edge device to enable traffic. Similarly, taking a redundant connection into use means additional requirements, in particular for routing protocols. In addition to these, some of Funet's services may require additional features from the edge devices. Some of the features are related to the ensuring, securing, monitoring, logging and management of the operations; they are not mandatory but may still be useful.

7.1. Funet Primary Connection

For the **Funet primary connection**, the device **must have** the following features:

- **IPv4 unicast routing** (mandatory)
- **Ipv6 unicast routing** [RFC2460] (mandatory)
 - IANA ran out of IPv4 addresses in early 2011
 - In order to retain the quality of service, packet forwarding must be done in hardware or at similar performance as IPv4
- **1 GE or 10 GE** interfaces [IEEE802.3] (mandatory)
 - One fibre port for Funet connection, preferably with replaceable optics
 - Connection type depending on the required data transfer capacity
 - In some cases, support for coloured CWDM or DWDM optics [CWDM] [DWDM]

7.2. Funet Secondary Connection

In addition to the features of the **Funet primary connection**, the following are required for the **Funet secondary connection**:

- **BGPv4** [RFC4271] (**mandatory**)
 - IPv4 and IPv6 routing information exchange
 - For multicast, see the separate section on MBGP
- **OSPF/OSPFv3 [RFC2328] [RFC5340] or IS-IS [RFC5308]** (**useful**)
 - For redundant connection of several Funet edge devices and intranet routers
- **HSRP/VRRP** [RFC5798] (**additional feature**)
 - Towards the campus LAN, if edge devices are duplexed
 - Enables the switchover of traffic to the backup route with the help of a virtual gateway address
- **1 GE or 10 GE** interfaces (**mandatory**)
 - One fibre port for Funet connection and at least one for connecting the edge devices
 - Connection type depending on the required data transfer capacity
 - In some cases, support for coloured CWDM or DWDM optics [CWDM][DWDM]

1.1 7.3. Multicast

The following features are required for multicast (e.g. Funet IPTV):

- **Static multicast routing or MBGP** [RFC4760] (**mandatory**)
 - Depending on the need for redundant routing, either static or dynamic multicast routing
- **PIM-SM [RFC4601]** (**mandatory**)
 - IPv4 and IPv6 ASM multicast for routing to Funet and other edge devices; signals the active senders and receivers to the RP
 - Support for IPv6 Embedded RP [RFC3956]
- **IGMPv2 / MLDv1 [RFC2236] [RFC2710]** (**mandatory**)
 - For IPv4 and IPv6 ASM multicast to the LAN, maintains and forwards the state information of senders and receivers
 - **IGMP snooping** and **MLD snooping** [RFC4541] required for the switches so that the traffic does not echo to all ports.
- **PIM-SSM [RFC4607], IGMPv3 / MLDv2 [RFC3376] [RFC3810] [RFC5186]** (**additional feature**)
 - Correspondingly, for SSM multicast for edge devices and IGMPv3/MLDv2 snooping for switches
- **MSDP [RFC3618] [RFC4611]** (**additional feature**)
 - For the advertisement of global multicast sessions
 - Funet's MSDP service is also in use
- **Anycast RP with MSDP or PIM [RFC4610]** (**additional feature**)
 - For RP duplexing
- **Access control lists for PIM/MSDP/IGMP/MLD protocols** (**additional feature**)
 - For filtering multicast group information

7.4. Light Paths

- A separate port is required for each light path (1GE or 10 GE)
- Typically, support for **CWDM** optics is required (1 GE or 10 GE) [CWDM]
- CWDM optics are required, if existing fibre pairs are utilised (Funet connection)
 - Passive CWDM muxes are installed on the fibre pairs

7.5. Other Features

The following edge device features should also be taken into consideration:

7.5.1. Fault Tolerance, Duplexed Components

- Power sources (at least two, the device must remain operational if one breaks down)
- Fan modules
- Routing module
 - interruption-free operation during routing module disruptions (switchover to the second routing module)
 - interruption-free updates
- “Hot-swap” feature for component replacement

7.5.2. Maintenance and Management Features

- Secure maintenance connection (SSH)
- Log sending to an external syslog server
- SNMPv3 network monitoring interface
- 64-bit counters for ports (32-bit versions will easily roll over)
- IPFix/NetFlow/sFlow or corresponding IP traffic logging and analysis feature
- Separate management connection via own VLAN or a physical port
- Port/VLAN traffic mirroring (Port Mirroring/Span Port) to a port or over the network.
- Possibility of saving the full configuration in an ASCII file

7.5.3. Device Support and Software

- Service agreements and response times during disruptions
- Support for software updates, “roadmap” for future features
- Manufacturer’s support during disruptions (phone, e-mail, web, local representative)
- Licences, additional feature-specific licences
- Support for device manufacturer independent optics

7.5.4. Connection of the Edge Devices to the Switch Infrastructure (Layer 2)

- Link duplexing
 - With LAG, LACP protocol [IEEE802.1AX]
 - MLAG, MC-LAG or corresponding, aggregation into several physical devices
 - Spanning Tree (802.1d) for link verification
 - Rapid STP [IEEE802.1D]
 - Multiple STP [IEEE802.1Q]
- Virtual LAN (VLAN) support [IEEE802.1Q]

7.5.5. Protections in the Switch Infrastructure (Layer 2)

- **DHCP snooping**
 - Prevents queries to so-called “rogue” DHCP servers, such as ADSL modems or WLAN access points “inadvertently” connected to the network.
 - Maintains a list of the ports to which computers are connected to.
 - Ensures that the device only uses the IP addresses given by the DHCP server.
- **IPv6 RA Guard and DHCPv6 snooping** [RFC6105]
 - Prevents extraneous IPv6 Router Advertisements.
 - Can also be implemented by port-based filtering of “rogue” RA messages and DHCPv6 servers in the switches
- **Port security**
 - A port can be locked to work with only certain MAC addresses.
 - 802.1X port-specific authentication
- **ARP inspection/IP source guard**
 - A means to ensure that the IP address generating traffic belongs to the right device.
- **L2 access control lists**
 - Access control lists on switch ports
- **Private VLAN support**

8. References

- [RFC2236] RFC 2236, Internet Group Management Protocol, Version 2, <http://tools.ietf.org/html/rfc2236>
- [RFC2328] RFC 2328, OSPF Version 2, <http://tools.ietf.org/html/rfc2328>
- [RFC2460] RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, <http://tools.ietf.org/html/rfc2460>
- [RFC2710] RFC 2710, Multicast Listener Discovery (MLD) for IPv6, <http://tools.ietf.org/html/rfc2710>
- [RFC2827] BCP 38, RFC 2827, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, <http://tools.ietf.org/html/rfc2827>
- [RFC3376] RFC 3376, Internet Group Management Protocol, Version 3, <http://tools.ietf.org/html/rfc3376>
- [RFC3618] RFC 3618, Multicast Source Discovery Protocol (MSDP), <http://tools.ietf.org/html/rfc3618>
- [RFC3654] RFC 3654, Requirements for Separation of IP Control and Forwarding, <http://tools.ietf.org/html/rfc3654>
- [RFC3704] BCP 84, RFC 3704, Ingress Filtering for Multihomed Networks, <http://tools.ietf.org/html/rfc3704>
- [RFC3810] RFC 3810, Multicast Listener Discovery Version 2 (MLDv2) for IPv6, <http://tools.ietf.org/html/rfc3376>
- [RFC3956] RFC 3956, Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address, <http://tools.ietf.org/html/rfc3956>
- [RFC4271] RFC 4271, A Border Gateway Protocol 4 (BGP-4), <http://tools.ietf.org/html/rfc4271>
- [RFC4541] RFC 4541, Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches, <http://tools.ietf.org/html/rfc4541>
- [RFC4601] RFC 4601, Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised), <http://tools.ietf.org/html/rfc4601>
- [RFC4607] RFC 4607, Source-Specific Multicast for IP, <http://tools.ietf.org/html/rfc4607>
- [RFC4610] RFC 4610, Anycast-RP Using Protocol Independent Multicast (PIM), <http://tools.ietf.org/html/rfc4610>
- [RFC4611] RFC 4611, Multicast Source Discovery Protocol (MSDP) Deployment Scenarios, <http://tools.ietf.org/html/rfc4611>
- [RFC4732] RFC 4732, Internet Denial-of-Service Considerations, <http://tools.ietf.org/html/rfc4732>
- [RFC4760] RFC 4760, Multiprotocol Extensions for BGP-4, <http://tools.ietf.org/html/rfc4760>
- [RFC5186] RFC 5186, Internet Group Management Protocol Version 3 (IGMPv3) / Multicast Listener Discovery Version 2 (MLDv2) and Multicast Routing Protocol Interaction, <http://tools.ietf.org/html/rfc5186>
- [RFC5308] RFC 5308, Routing IPv6 with IS-IS, <http://tools.ietf.org/html/rfc5308>
- [RFC5340] RFC 5340, OSPF for IPv6, <http://tools.ietf.org/html/rfc5340>
- [RFC5575] RFC 5575, Dissemination of Flow Specification Rules, <http://tools.ietf.org/search/rfc5575>

- [RFC5635] RFC 5635, Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF), <http://tools.ietf.org/html/rfc5635>
- [RFC5798] RFC 5798, Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6, <http://tools.ietf.org/html/rfc5798>
- [RFC6105] RFC 6105, IPv6 Router Advertisement Guard, <http://tools.ietf.org/html/rfc6105>
- [CPP] IETF Draft, draft-ietf-opsec-protect-control-plane-06, Protecting The Router Control Plane, <http://tools.ietf.org/html/draft-ietf-opsec-protect-control-plane-06>
- [IEEE802.1AX] IEEE 802.1AX-2008, IEEE Standard for Local and Metropolitan Area Networks - Link Aggregation, <http://standards.ieee.org/getieee802/download/802.1AX-2008.pdf>

Glossary

ADSL	Asymmetric Dynamic Subscriber Line
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
BCP	Binary Communications Protocol
BGP	Border Gateway Protocol
CWDM	Coarse Wavelength Division Multiplexing
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DWDM	Dense Wavelength Division Multiplexing
FIB	Forwarding Information Base
HSRP	Hot Standby Router Protocol
IANA	Internet Assigned Numbers Authority
IGMP	Internet Group Management Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IS-IS	Intermediate System to Intermediate System
IPTV	IP Television
L2	Layer 2
LACP	Link Aggregation Control Protocol
LAG	Local Address Group
LAN	Local Area Network
MAC	Media Access Control
MBGP	Multiprotocol BGP
MC-LAG	Multi-Chassis Link Aggregation Group
MLAG	Multi-Chassis Link Aggregation Group
MLD	Multicast Listener Discovery
MSDP	Multicast Source Discovery Protocol
OSPF	Open Shortest-Path First
PIM	Protocol Independent Multicast
PIM-SM	Protocol Independent Multicast – Source Mode
PIM-SSM	Protocol Independent Multicast – Source Specific Multicast
PPS	Packet Per Second
QoS	Quality of Service
R&E	Research and Education
RA	Router Advertisement

RFC	Request for Comments
RIB	Routing Information Base
RP	Rendezvous Point
RSTP	Rapid STP
SNMP	Simple Network Management Protocol
SSH	Secure Shell
STP	Spanning Tree Protocol
VLAN	Virtual LAN
VRRP	Virtual Router Redundancy Protocol
WLAN	Wireless LAN

