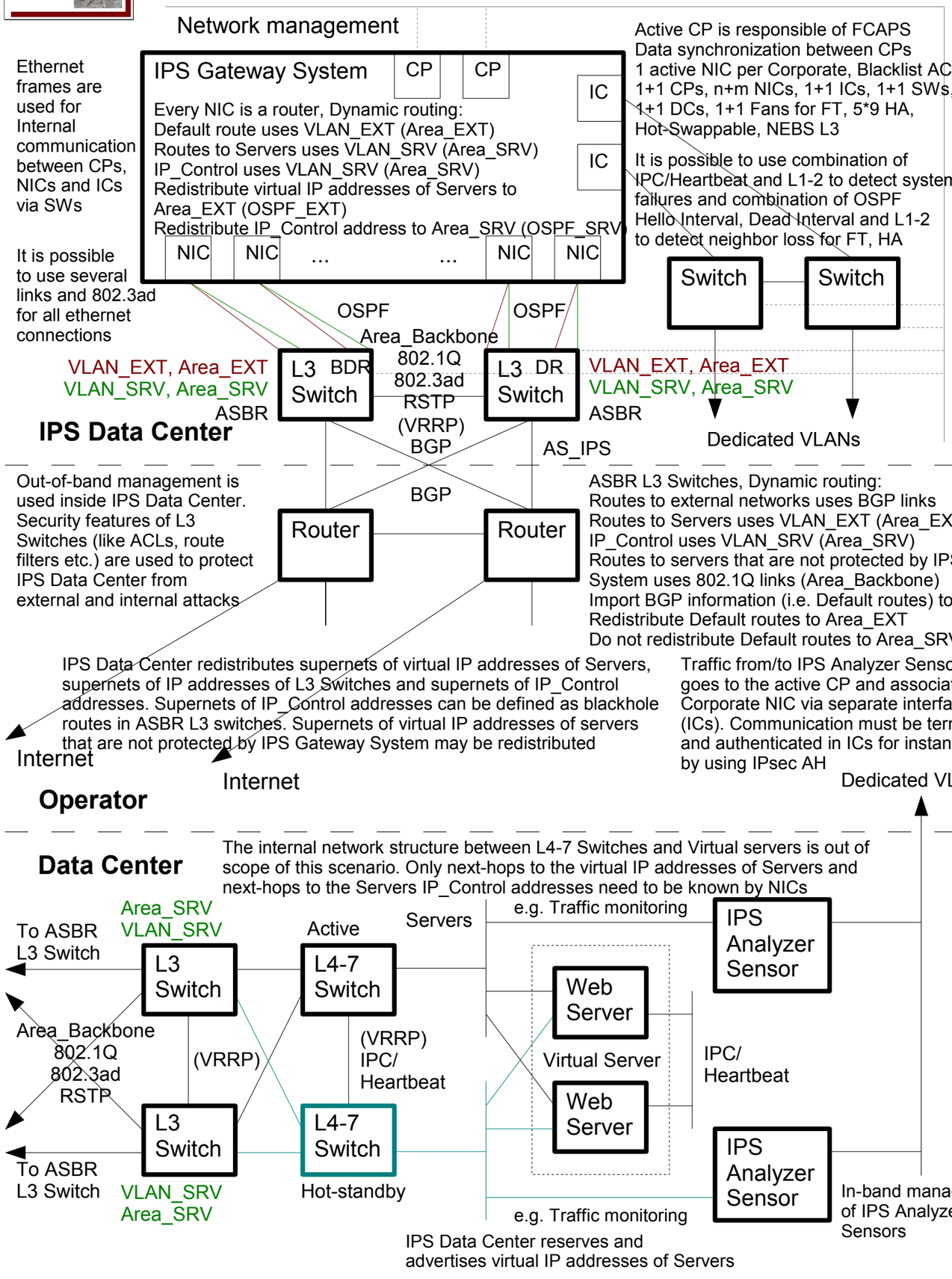
IPS Data Center - Scenario 2: Web Server[1] in Data Center

IPS Data Center can be connected to the Operator's Site Backbone Routers or Data Center Distribution Gateways



It is possible to locate several IPS Gateway Systems and additional L3 Switches to one IPS Data Center. Hierarchical network architecture can be implemented by using standard L2 switching and L3 routing technologies with VLANs

Every NIC must support multiple routing instances for OSPF routing protocol to separate redistribution of IP subnets. A NIC has VLAN_EXT interfaces connected to OSPF area Area_EXT handled by OSPF routing instance OSPF_EXT and VLAN_SRV interfaces connected to OSPF area Area_SRV handled by OSPF routing instance OSPF_SRV. Thus virtual IP addresses of Servers can be redistributed to area Area_EXT without redistributing them to area Area_SRV and IP_Control address can be redistributed to area Area_SRV without redistributing them to Area_EXT

L3 Switches must support multiple modular routing instances

Every NIC is a router, Policy based routing:
if src=IP_Control and proto=Controls then DiffServ (and 802.1p) marking
if dest=Servers and proto=Web then DiffServ (and 802.1p) marking

It is possible to use several VLANs for external networks and several VLANs for Servers

It is possible to configure OSPF so that the IPS Gateway System including L3 Switches can be reasonably implemented. Backbone, stub and totally stubby areas, multiple OSPF routing instances, route summarization, route filters, route maps etc. can be used for this purpose. Route filtering features of NICs can be used instead of not redistributing Default routes to Area_SRV

It is possible to use VRRP and static routing instead of OSPF. VRRP may also be used to monitor interfaces of L3 Switches

There is IP control traffic between Servers and associated NICs in IPS Gateway System. A NIC monitors that Virtual servers are reachable by using ping polling and triggers. In the case of failure connections that are attached to Virtual servers (or entire NIC) are deactivated and failover is performed

IP control traffic packets have priority over other IP packets to guarantee that monitoring of Servers reachability can be implemented during service attacks or network congestion without performing unnecessary failovers of NICs

Traffic shaping in NIC can be used to limit the volume and rate of clients' traffic to Servers for instance based on the capacity of L4-7 Switches and Virtual servers. Traffic shaping is implemented by using combination of token bucket and leaky bucket algorithms

QoS from external networks to Servers is implemented by using over-provisioning in VLAN_EXT interfaces, by shaping clients' traffic to Servers and by using combination of DiffServ and 802.1p in VLAN_SRV interfaces. QoS from Servers to external networks is implemented by using over-provisioning in 802.1Q interfaces of L3 Switches

Several queuing algorithms can be used: FIFO or WFQ (based on FQ) in VLAN_EXT interfaces and Priority or Class based WFQ (based on DSCP) in VLAN_SRV interfaces

DiffServ and 802.1p marking can be used to guarantee different QoS levels for different services (http, smtp, dns, ldap, ftp etc.)

Traffic Flows inside NIC

Inbound VLAN_EXT:
Queuing

Blacklist ACL

Traffic shaping
DiffServ marking
Forwarding based on route selection (Linux based route cache, RPDB and RTs)

Outbound VLAN_SRV:
Queuing
802.1p marking (based on DSCP)
Forwarding

Inbound VLAN_SRV:
Queuing
ACL

Traffic shaping
Forwarding based on route selection (Linux based route cache, RPDB and RTs)

Outbound VLAN_EXT:
Queuing
Forwarding

There is a bidirectional communication between active CP and every NIC. ICs are used for secure connections to the IPS Analyzer Sensors. Active CP is responsible of Fault management including alarms, logs, system failures and NIC failovers, Configuration management including maintaining and pushing configuration to the NICs, Accounting management including administration and gathering statistics of system components, Performance management including collecting performance data and Security management including controlling access to the system.

L3 Switches, Dynamic routing:
Routes to external networks uses 802.1Q links (Area_Backbone)
Route to IP_Control addresses uses 802.1Q links (VLAN_SRV, Area_SRV)
Redistribute virtual IP addresses of Servers to Area_SRV
Redistribute virtual IP addresses of servers that are not protected by IPS Gateway System to Area_Backbone
Redistribute Servers IP_Control addresses to Area_SRV
Do not redistribute Default routes to Area_SRV

L3 and L4-7 Switches are controlled by IPS Data Center / Operator
Traffic between NICs' IP_Control addresses and Servers IP_Control addresses goes via ASBR L3 Switches using VLAN_SRV (Area_SRV)
Traffic from external networks to Servers goes via IPS Gateway System using BGP links, Area_Backbone, VLAN_EXT (Area_EXT) and VLAN_SRV (Area_SRV)
Traffic from Servers to external networks goes via ASBR L3 Switches using Area_Backbone
Traffic between external networks and servers that are not protected by IPS Gateway System goes via L3 Switches using Area_Backbone

L3 Switches, Policy based routing:
If it is required that also traffic from Servers to external networks goes via IPS Gateway System using VLAN_SRV (Area_SRV), VLAN_EXT (Area_EXT), Area_Backbone and BGP links then policies must be configured in L3 Switches for every protected Servers. In this case also QoS including traffic shaping can be implemented.
if src=Servers and proto=Web then DiffServ (and 802.1p) marking
if src=Servers then next-hop=IP address of associated NIC's VLAN_SRV interfaces

Source of terminology: e.g. www.wikipedia.org

Version 1.0.6 © 23.5.2007, Mika.Panhelainen@iki.fi

1) IPS Gateway System can also be used to protect other public services like smtp, dns, ldap, ftp etc. It may be possible to implement an IPS Analyzer Sensor functionality inside an associated Corporate NIC. In this case a dedicated VLAN connection to the Data Center via separate interfaces (ICs) is not needed