UCL

Université
catholique
de Louvain

Infrastructures de production du système d'information (SIPR)
Service Général du Système d'Information (SGSI)

Case study : UCL's computer network

Quentin Hunin
Network engineer

INGI2142
LLN - February 2018

About myself

Graduated from UCL in 2011

Network engineer at ING Belgium between 2011 and 2013

Network engineer at UCL since 2013

Agenda

- Some design considerations
- Some figures
- IP plan
- Core network
- External connections
- Data-centers
- Campus
- DHCP / DNS
- Monitoring and management tools
- Future

Design considerations

Applications give sense to IT infrastructures

but IT infrastructures make it possible.

Computer networks belong to the foundations.

Design considerations

- Optimal technical solution
- Cost and time
- History
- Existing agreements
- Management
- Compliancy and legal constraints
- Public tender rules
- Maintenance cost
- Staffing

…

Some figures

6 000 staff members

30 000 students

6 geographical sites (LLN, Woluwe, Saint-Gilles, Mons, Tournai, Charleroi)

100+ buildings

Tens of partners depending on our IT (non-profits organizations, hospitals, schools,…)

Some IT figures

3 main data-centers / 500 servers / 150 TB of storage

10 Gigabit connectivity towards research networks

5 Gigabit commercial bandwidth

7 core L3 switches

560 Ethernet access and distribution switches

28.000 network outlets

950 WiFi access points supporting up to 13.500 clients

30 kms of fiber cables

How do we connect

What we connect and power









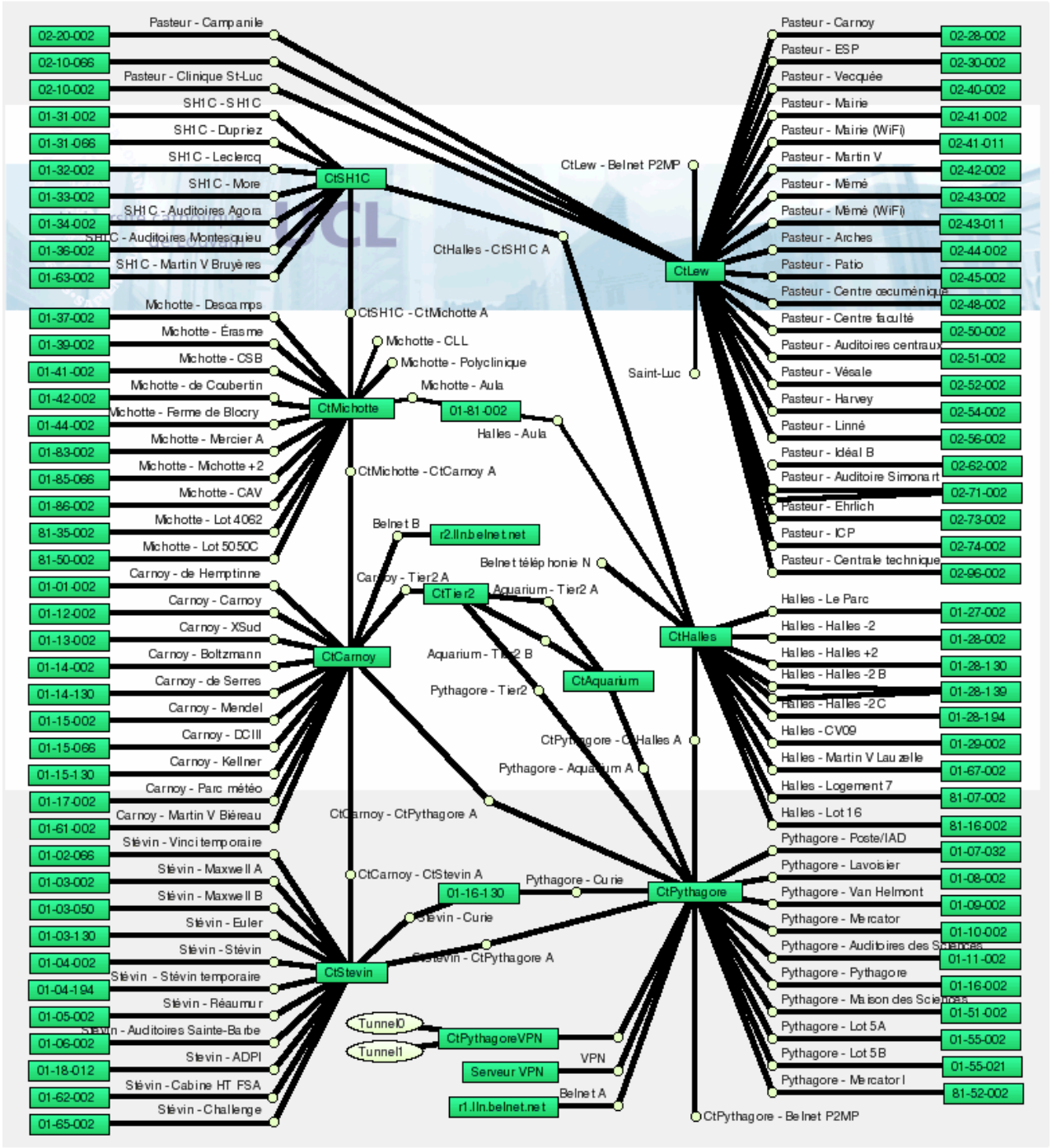








The big picture


Pasteur - Campanile
02-20-002
02-10-066
Pasteur - Clinique St-Luc
02-10-002
SH1C - SH1C
01-31-002
SH1C - Dupriez
01-31-066
SH1C - Leclercq
01-32-002
SH1C - More
01-33-002
SH1C - Auditoires Agora
01-34-002
SH1C - Auditoires Montesquieu
01-36-002
SH1C - Martin V Bruyères
01-63-002
CtSH1C
CtLew - Belnet P2MP
CtHalles - CtSH1C A
CtLew
Pasteur - Carnoy
Pasteur - ESP
Pasteur - Vecquée
Pasteur - Mairie
Pasteur - Mairie (WiFi)
Pasteur - Martin V
Pasteur - Mêmé
Pasteur - Mêmé (WiFi)
Pasteur - Arches
Pasteur - Patio
Pasteur - Centre oecuménique
Pasteur - Centre faculté
Pasteur - Auditoires centraux
Pasteur - Vésale
Pasteur - Harvey
Pasteur - Linné
Pasteur - Idéal B
Pasteur - Auditoire Simonart
Pasteur - Ehrlich
Pasteur - ICP
Pasteur - Centrale technique
02-28-002
02-30-002
02-40-002
02-41-002
02-41-011
02-42-002
02-43-002
02-43-011
02-44-002
02-45-002
02-48-002
02-50-002
02-51-002
02-52-002
02-54-002
02-56-002
02-62-002
02-71-002
02-73-002
02-74-002
02-96-002
Saint-Luc
Michotte - Descamps
01-37-002
Michotte - Érasme
01-39-002
Michotte - CSB
01-41-002
Michotte - de Coubertin
01-42-002
Michotte - Ferme de Blocry
01-44-002
Michotte - Mercier A
01-83-002
Michotte - Michotte +2
01-85-066
Michotte - CAV
01-86-002
Michotte - Lot 4062
81-35-002
Michotte - Lot 5050C
81-50-002
CtSH1C - CtMichotte A
Michotte - CLL
Michotte - Polyclinique
Michotte - Aula
CtMichotte
01-81-002
Halles - Aula
CtMichotte - CtCarnoy A
Belnet B
r2.lln.belnet.net
Belnet téléphonie N
Carnoy - de Hemptinne
01-01-002
Carnoy - Carnoy
01-12-002
Carnoy - XSud
01-13-002
Carnoy - Boltzmann
01-14-002
Carnoy - de Serres
01-14-130
Carnoy - Mendel
01-15-002
Carnoy - DCIII
01-15-066
Carnoy - Kellner
01-15-130
Carnoy - Parc météo
01-17-002
Carnoy - Martin V Biéreau
01-61-002
Carnoy - Tier2 A
CtTier2
Aquarium - Tier2 A
Aquarium - Tier2 B
Pythagore - Tier2
CtAquarium
CtCarnoy
CtPythagore - CtHalles A
Pythagore - Aquarium A
CtCarnoy - CtPythagore A
CtHalles
Halles - Le Parc
Halles - Halles -2
Halles - Halles +2
Halles - Halles -2 B
Halles - Halles -2 C
Halles - CV09
Halles - Martin V Lauzelle
Halles - Logement 7
Halles - Lot 16
01-27-002
01-28-002
01-28-130
01-28-139
01-28-194
01-29-002
01-67-002
81-07-002
81-16-002
Stévin - Vinci temporaire
01-02-066
Stévin - Maxwell A
01-03-002
Stévin - Maxwell B
01-03-050
Stévin - Euler
01-03-130
Stévin - Stévin
01-04-002
Stévin - Stévin temporaire
01-04-194
Stévin - Réaumur
01-05-002
Stevin - Auditoires Sainte-Barbe
01-06-002
Stevin - ADPI
01-18-012
Stévin - Cabine HT FSA
01-62-002
Stévin - Challenge
01-65-002
CtCarnoy - CtStevin A
01-16-130
Stevin - Curie
Stevin - CtPythagore A
CtStevin
Pythagore - Curie
CtPythagore
Pythagore - Poste/IAD
Pythagore - Lavoisier
Pythagore - Van Helmont
Pythagore - Mercator
Pythagore - Auditoires des Sciences
Pythagore - Pythagore
Pythagore - Maison des Sciences
Pythagore - Lot 5A
Pythagore - Lot 5B
Pythagore - Mercator I
01-07-032
01-08-002
01-09-002
01-10-002
01-11-002
01-16-002
01-51-002
01-55-002
01-55-021
81-52-002
Tunnel0
Tunnel1
CtPythagoreVPN
VPN
Serveur VPN
Belnet A
r1.lln.belnet.net
CtPythagore - Belnet P2MP

IP prefixes

130.104.0.0/16

192.135.167.0/23

193.191.171.0/24

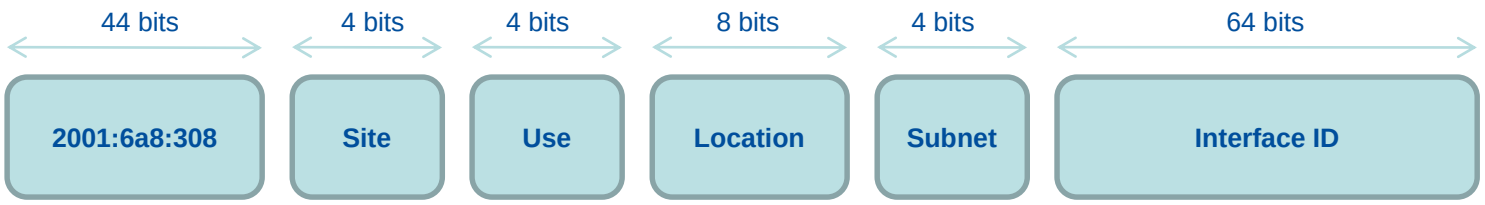
→ no NAT needed

2001:6a8:3080::/44

IPv4 addressing plan

- No addressing plan at that time
- Started with a first asked first served assignment

IPv6 addressing plan



Encode information inside the prefix to:

have smaller routing tables.

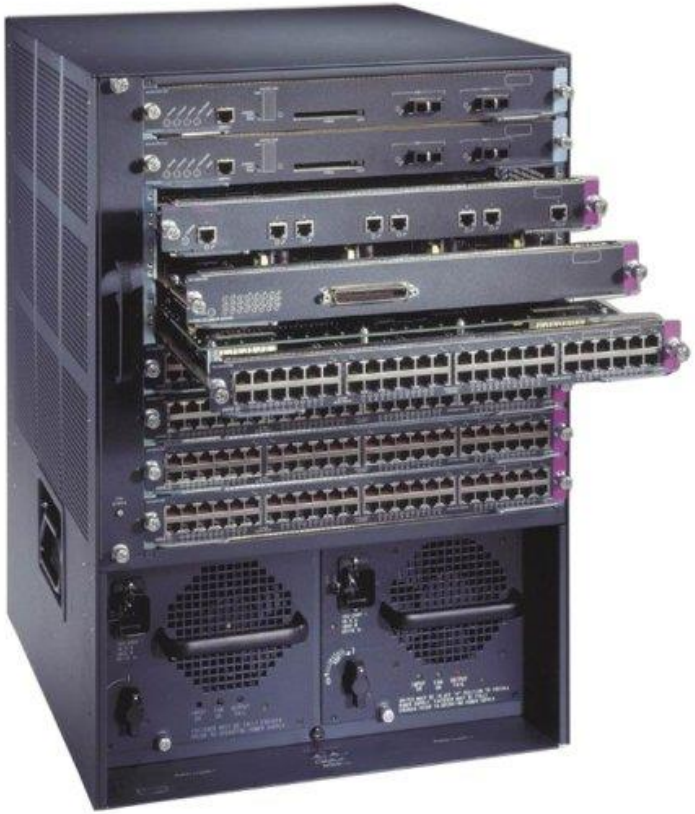
make filtering rules easier and more readable

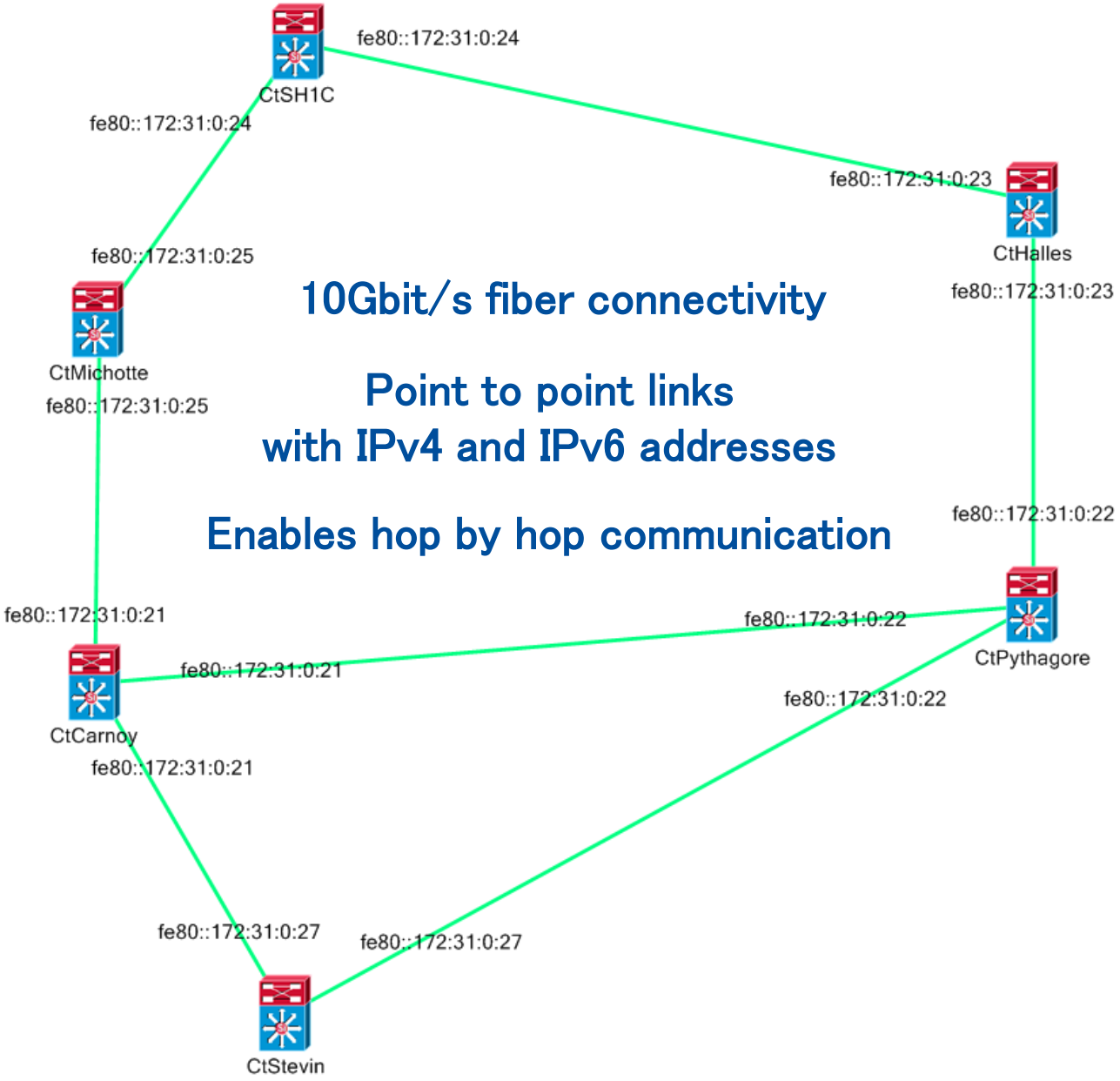
Core network

- 10 Gbit/s inter router links
- Dual stack IPv4 / IPv6.
- Supports unicast and multicast traffic forwarding

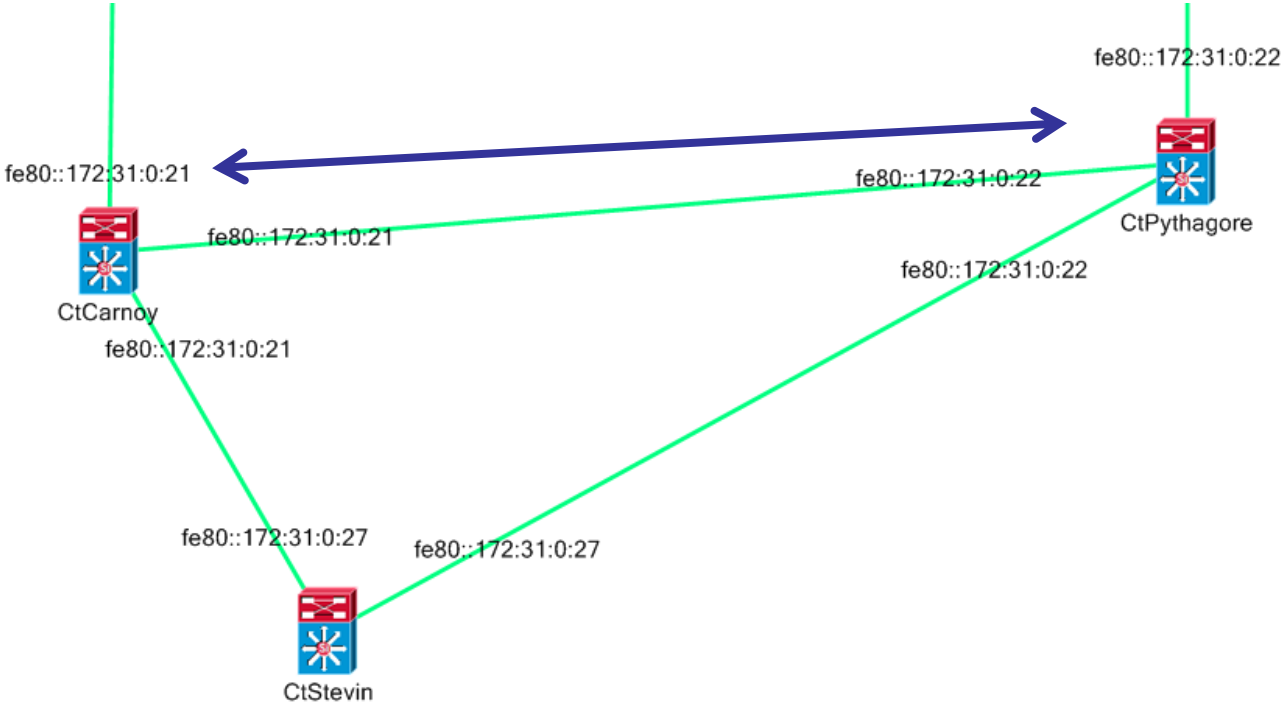
Core network

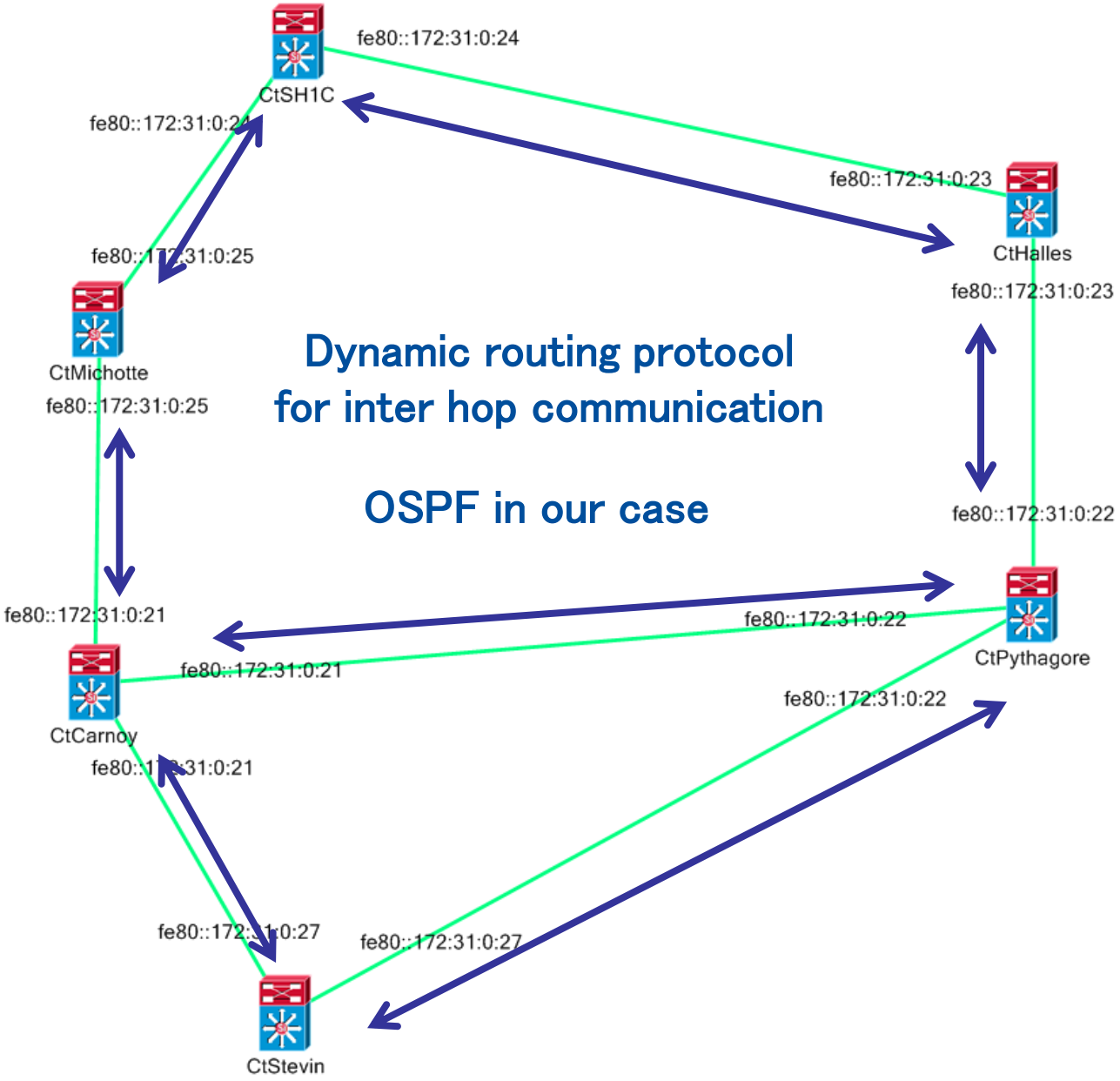
Cisco 6509-E

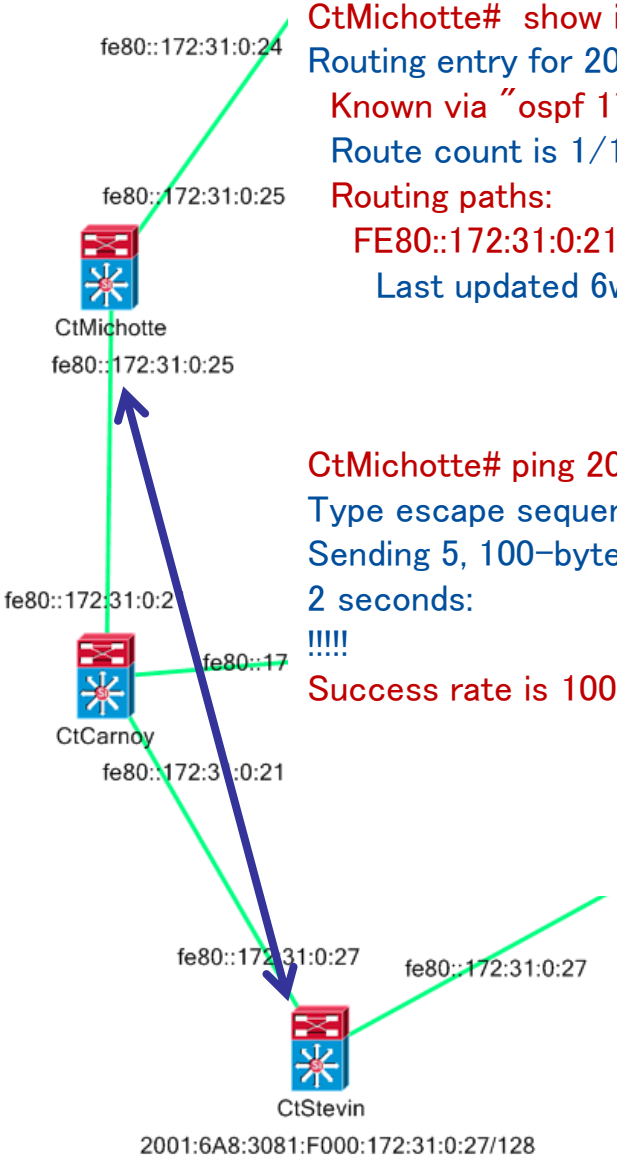



fe80::172:31:0:24
CtSH1C
fe80::172:31:0:24
fe80::172:31:0:23
CtHalles
fe80::172:31:0:25
CtMichotte
fe80::172:31:0:25
fe80::172:31:0:23
10Gbit/s fiber connectivity
Point to point links
with IPv4 and IPv6 addresses
Enables hop by hop communication
fe80::172:31:0:22
fe80::172:31:0:21
fe80::172:31:0:22
CtPythagore
fe80::172:31:0:21
fe80::172:31:0:22
CtCarnoy
fe80::172:31:0:21
fe80::172:31:0:27
fe80::172:31:0:27
CtStevin

```
CtPythagore# ping FE80::172:31:0:21
Output Interface: Vlan981
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::172:31:0:21, timeout is 2 seconds:
Packet sent with a source address of FE80::172:31:0:22%Vlan981
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```




fe80::172:31:0:24
CtSH1C
fe80::172:31:0:24
fe80::172:31:0:23
CtHalles
fe80::172:31:0:25
CtMichotte
fe80::172:31:0:25
fe80::172:31:0:23
Dynamic routing protocol
for inter hop communication
OSPF in our case
fe80::172:31:0:22
fe80::172:31:0:21
fe80::172:31:0:22
CtPythagore
fe80::172:31:0:21
fe80::172:31:0:21
fe80::172:31:0:22
CtCarnoy
fe80::172:31:0:21
fe80::172:31:0:27
fe80::172:31:0:27
CtStevin



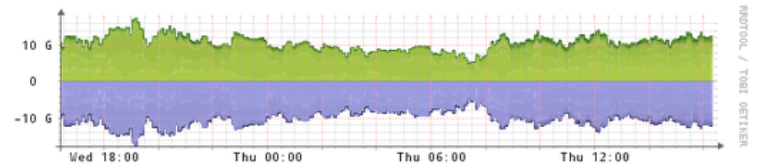

```
CtMichotte#  show ipv6 route 2001:6A8:3081:F000:172:31:0:27
Routing entry for 2001:6A8:3081:F000:172:31:0:27/128
  Known via "ospf 1", distance 110, metric 3, type intra area
  Route count is 1/1, share count 0
  Routing paths:
    FE80::172:31:0:21, Vlan985
      Last updated 6w2d ago
```

```
CtMichotte# ping 2001:6A8:3081:F000:172:31:0:27
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:6A8:3081:F000:172:31:0:27, timeout is
2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
```

Cisco IOS Software, s2t54 Software (s2t54-IPSERVICESK9-M), Version 15.1(2)SY7, RELEASE SOFTWARE (fc4) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2016 by Cisco Systems, Inc. Compiled Sun 13-Mar-16 07:14 by prod_rel_team

Hardware	Cisco 6509 (WS-C6509-E)
Operating system	Cisco IOS 15.1(2)SY7 (IPSERVICESK9)
System name	ctpythagore.sri.ucl.ac.be
Contact	UCL/SRI, +32 (10) 47 2611, sri@sri.ucl.ac.be
Serial	SMC09210001
Uptime	1 year, 313 days, 17m 17s
Last reboot	2016-04-01 15:02:46

Ports



255 235 2 18

Te2/1, Te2/2, Te2/3, Te2/4, Te2/5, Te2/6, Te2/7, Te2/8, Te2/9, Te2/10, Te2/11, Te2/12, Te2/13, Te2/14, Te2/15, Te2/16, Te5/4, Te5/5, NDE_0, Gi1/1, Gi1/2, Gi1/3, Gi1/4, Gi1/5, Gi1/6, Gi1/7, Gi1/8, Gi1/9, Gi1/10, Gi1/11, Gi1/12, Gi1/13, Gi1/14, Gi1/15, Gi1/16, Gi1/17, Gi1/18, Gi1/19, Gi1/20, Gi1/21, Gi1/22, Gi1/23, Gi1/24, Gi5/1, Gi5/2, Gi5/3, Gi8/1, Gi8/2, Gi8/3, Gi8/4, Gi8/5, Gi8/6, Po24, Vlan1, Vlan99, Vlan134, Vlan151, Vlan196, Vlan200, Vlan201, Vlan202, Vlan203, Vlan207, Vlan208, Vlan209, Vlan211, Vlan212, Vlan213, Vlan214, Vlan216, Vlan217, Vlan218, Vlan219, Vlan220, Vlan221, Vlan222, Vlan223, Vlan224, Vlan225, Vlan226, Vlan227, Vlan228, Vlan230, Vlan231, Vlan232, Vlan233, Vlan234, Vlan235, Vlan236, Vlan237, Vlan238, Vlan239, Vlan240, Vlan241, Vlan242, Vlan243, Vlan244, Vlan245, Vlan246, Vlan247, Vlan248, Vlan249, Vlan250, Vlan252, Vlan253, Vlan254, Vlan255, Vlan256, Vlan257, Vlan258, Vlan259, Vlan260, Vlan261, Vlan262, Vlan264, Vlan265, Vlan266, Vlan267, Vlan268, Vlan269, Vlan270, Vlan271, Vlan272, Vlan273, Vlan274, Vlan275, Vlan276, Vlan277, Vlan278, Vlan279, Vlan280, Vlan281, Vlan282, Vlan283, Vlan298, Vlan299, Vlan303, Vlan307, Vlan308, Vlan309, Vlan310, Vlan449, Vlan484, Vlan808, Vlan809, Vlan811, Vlan812, Vlan813, Vlan814, Vlan815, Vlan816, Vlan817, Vlan818, Vlan819, Vlan820, Vlan821, Vlan822, Vlan824, Vlan826, Vlan828, Vlan829, Vlan830, Vlan831, Vlan833, Vlan836, Vlan837, Vlan838, Vlan839, Vlan842, Vlan843, Vlan844, Vlan845, Vlan848, Vlan850, Vlan851, Vlan859, Vlan873, Vlan874, Vlan875, Vlan876, Vlan877, Vlan879, Vlan881, Vlan886, Vlan887, Vlan888, Vlan889, Vlan891, Vlan894, Vlan895, Vlan896, Vlan897, Vlan898, Vlan920, Vlan921, Vlan922, Vlan923, Vlan924, Vlan925, Vlan926, Vlan927, Vlan928, Vlan929, Vlan981, Vlan982, Vlan983, Vlan988, Vlan989, Vlan991, Vlan992, Vlan1200, Vlan1201, Vlan1202, Vlan1203, Vlan1204, Vlan1205, Vlan1206, Vlan1207, Vlan1208, Vlan1209, Vlan1210, Vlan1211, Vlan1296, Vlan1297, Vlan1873, Vlan1981, Vlan1982, Vlan1983, Vlan1988, Vlan1989, Vlan2981, Vlan2982, Vlan2983, Vlan3204, Vlan3205, Vlan3206, Vlan3210, Vlan3215, Vlan3251, Vlan3891, Vlan3893, Po360, Tu0, Tu1, Tu2, Tu11, Tu12, Lo0, Lo1, Lo2, Lo3, Lo11, Lo12, Null0, Control Plane

Processors

Routing Processor 5		17%
Module 1		9%
Module 2		46%

Memory

Module 1 (Processor)	58.6MB/181MB (32%)	122MB (68%)
Module 2 (Processor)	215MB/949MB (23%)	733MB (77%)
Routing Processor 5 (Processor)	324MB/1.41GB (22%)	1.1GB (78%)
Routing Processor 5 (I/O)	125MB/256MB (49%)	131MB (51%)

Storage

Boot Disk	282MB/977MB (29%)	694MB (71%)
CFC's Boot Flash	634kB/15.2MB (4%)	14.6MB (96%)

c6500/7600 Crossbar

Physical Slot 1			Crossbar	
Fabric 0	ok	20Gbps	Ingress 5%	Egress 0%
Physical Slot 2			DCEF	
Fabric 0	ok	20Gbps	Ingress 7%	Egress 2%
Fabric 1	ok	20Gbps	Ingress 2%	Egress 10%
Physical Slot 5				
Fabric 0	ok	20Gbps	Ingress 0%	Egress 2%
Fabric 1	ok	20Gbps	Ingress 3%	Egress 3%
Physical Slot 8				

Status Indicators

AC Power Supply, 3000 watt 1 - Power Supply 1 fa	true
AC Power Supply, 3000 watt 1 - Power Supply 1 in	true
AC Power Supply, 3000 watt 1 - Power Supply 1 po	true
AC Power Supply, 3000 watt 2 - Power Supply 2 fa	true
AC Power Supply, 3000 watt 2 - Power Supply 2 in	true
AC Power Supply, 3000 watt 2 - Power Supply 2 po	true

External connections

- Connects the internal network to the Internet through an ISP

  → BGP is used for this.

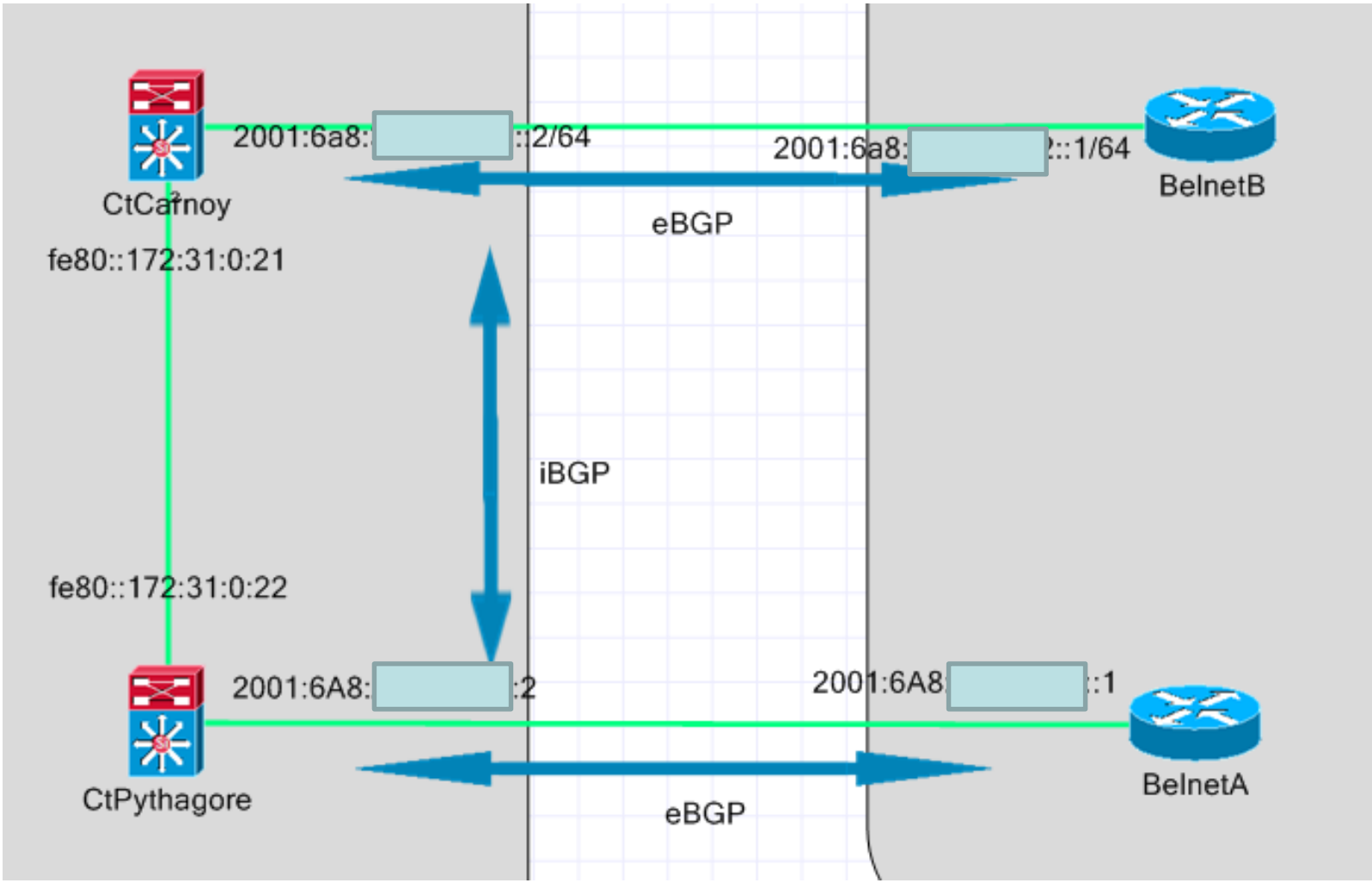
- Connects remote sites

  → L2 and L3 VPNs provided by ISP

  or directly over the Internet

- No DMZ in our case

Internet connectivity


2001:6a8:
::2/64
2001:6a8:
::1/64
BelnetB
CtCarnoy
eBGP
fe80::172:31:0:21
iBGP
fe80::172:31:0:22
2001:6A8:
:2
2001:6A8
::1
CtPythagore
BelnetA
eBGP

Internet connectivity

- Default route ::/0 announced by ISP on both BGP sessions
- UCL's prefix announced on both BGP session to ISP
- Local pref on both side to decide which link is active
- Filters on both side protect from incorrect announcements

CtCarnoy# show ip bgp ipv6 unicast

BGP table version is 3, local router ID is 193.191.X.Y

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,

x best-external, a additional-path, c RIB-compressed,

Origin codes: i - IGP, e - EGP, ? – incomplete

	Network	Next Hop	Metric	LocPrf	Weight	Path
r	**::/0**	**2001:6A8:3[redacted]2::1**				
			100		0	2611 i
r>i	**::/0**	**2001:6A8:A[redacted]:1**				
			0	**200**	0	2611 i

```
CtPythagore# show ipv6 route
IPv6 Routing Table - default - 82 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
B   ::/0 [20/0]
    via FE80::327C:5EFF:FE9F:3428, TenGigabitEthernet2/13
```

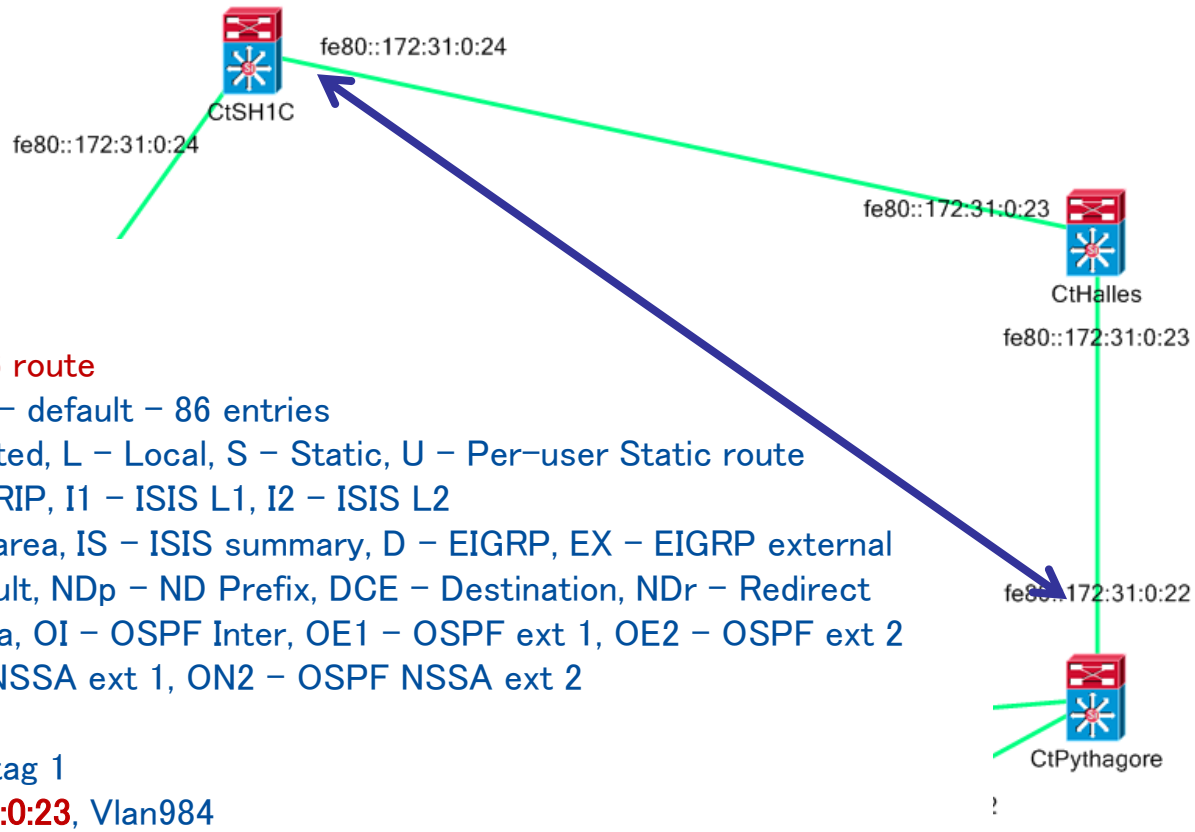
```
CtPythagore# ping 2001:4860:4860::8888 source Loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:4860:4860::8888, timeout is 2 seconds:
Packet sent with a source address of 2001:6A8:3081:F000:172:31:0:22
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/8 ms
```

Internet connectivity

- Other routers need to learn the default route
- Can be achieved by configuring BGP on each router

or

ask OSPF to generate and announce a default route




```
CtSH1C# show ipv6 route
IPv6 Routing Table - default - 86 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

OE2 ::/0 [110/50], tag 1
    via FE80::172:31:0:23, Vlan984
```

Security considerations

Make it robust by inserting static routes to null 0 on each router

ipv6 route 100::/8 null 0

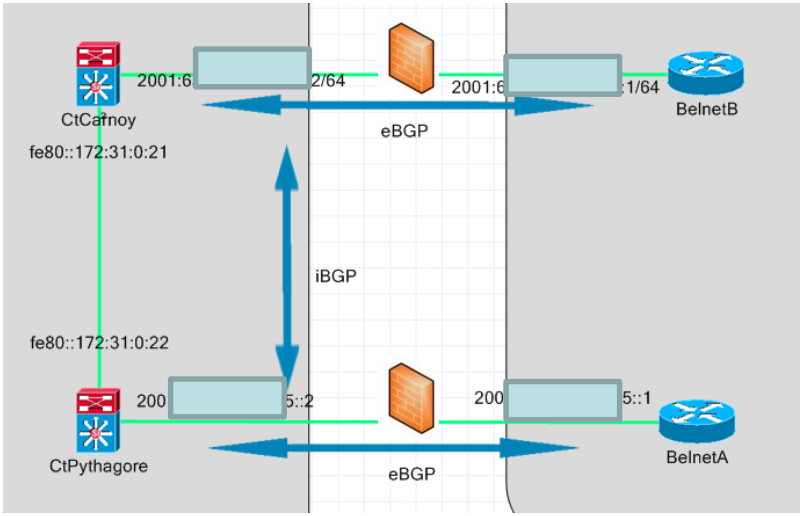
ipv6 route 2001:db8::/32 null 0

ipv6 route 2001:6a8:3080::/44 null 0

(…)

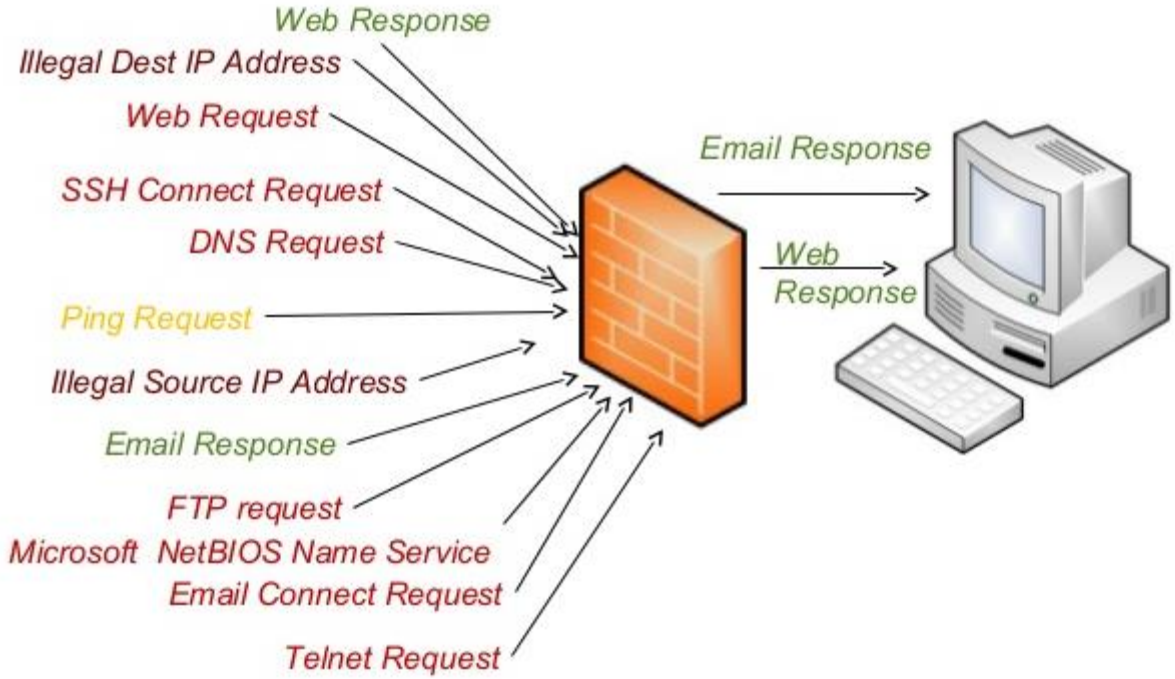
Security considerations (2)

- A big part of the IT threats come from the Internet
- Next generation firewalls protect the edge of the network



Security considerations (3)

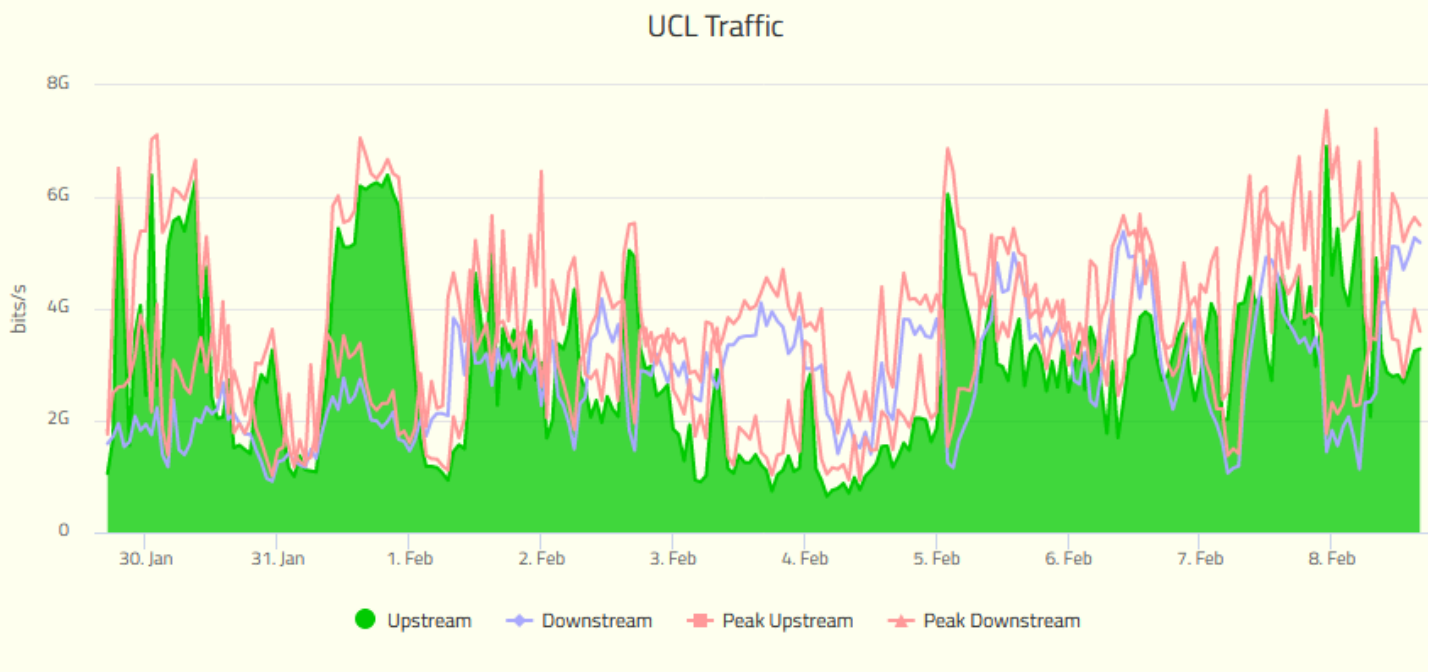
Packet Filter Firewall



Security considerations (4)

Next generation firewalls offer more granularity

Monitoring



	Max	Avg	Last
Upstream	6.91 GB	2.95 GB	3.25 GB
Downstream	5.38 GB	2.78 GB	5.27 GB
Peak Upstream	7.55 GB	3.77 GB	3.99 GB
Peak Downstream	6.06 GB	3.39 GB	5.64 GB

Data-centers

- Host business critical applications and data
- Security and high availability are very important
- Virtualization is a key component for efficiency, scalability and elasticity but imposes constraints to the network


PORTAIL / HEBERGEMENT
PORTAIL UCL
REDDOT CMS
HÉBERGEMENT UCL
ALFRESCO
TRANSVOL
FTP
SHAREPOINT
OWAPP
WORKFLOW
E-LEARNING
ICAMPUS
MOODLE
EPORTFOLIO
PODCAST
MAIL
POP EXCHG
IMAP EXCHG
OWA EXCHG
SMTP
SMTP-LISTES
MAILING LISTS
LISTES UCL
LISTES AUTRES
LISTES ETD
FILEMAKER
FMS
FMS2
FMS3
FMS4
FMS5
FMS6
FMS12
FMS13-0
FMS13-1
AUTHENTIFICATION
IDGLOBAL
ACTIVE DIRECTORY
SHIBBOLETH
ANNUAIRE
PROXY
PROXYSGSI
PROXY BIB
PROXY DIDAC
SIPS
EPC
OSIS
STUDIES
INSCRIPTION
HORAIRE
REAL
SRV FICHIERS
ALFRESCO
FS01A
FS02A
FS02B
FS03A
FS03B
FS03C
FS04A
FS04B
FS04C
FS05B
FS05C
FS06B
FS06C
FS08A
FS08B
FS08C
FS09A
SRV IMPRESSIONS
ANTENOR
PRN01
PRN02
PRN03
DIDACPRN
DPRN02
SAP
BIBLIOTHEQUES
PORTAIL BIB
VIRTUA
DIAL
HANDLE
SAP
PORTAIL ECPT
PORTAIL SAP
BWPGUI
HRPGUI
SAPGUI
PIP
SOLMAN
BUSINESS OBJECTS
ARCHIVAGE
DNS
NS1
NS2
NS3
DHCP
DHCP-1
DHCP-2
DHCPTEL-1
DHCPTEL-2
WIFI/VPN UCL
RADIUS1 PRS
RADIUS2 PRS
RADIUS1 LOGE
RADIUS2 LOGE
RADIUS1 EXT
RADIUS2 EXT
RADIUS1 EDUROAM
RADIUS2 EDUROAM
RADIUS1 VPN
RADIUS2 VPN

```
Device Status
          Name: PORTAIL UCL
      DNS Name: uclouvain.be.
       Address: 130.104.6.136
        Status: UP (Reachable since Feb 08, 02:26:31)
         Probe: HTTPS (port 443)
       Up Time: n/a
  Availability:           99.8 % (of 16 days, 0 hours, 52 minutes)
  TCP Failures:           0.03 % (of 23052 total attempts)
  Short-term Packet Loss:  0.0 % (of 100 last attempts)
  Recent Failure: 21 attempts at Feb 08, 02:06:01
  Response time:  150 msec
Recent Outages:
  02/08 02:06:01: DOWN for 20 minutes, 30 seconds
  02/06 14:41:28: DOWN for 1 minute, 0 seconds
  02/05 02:21:55: DOWN for 6 minutes, 30 seconds
  02/01 11:31:50: DOWN for 30 seconds
  02/01 02:24:49: DOWN for 3 minutes, 38 seconds
  01/30 02:24:44: DOWN for 3 minutes, 0 seconds
  01/29 02:26:42: DOWN for 36 seconds
  01/27 02:24:39: DOWN for 2 minutes, 56 seconds
  01/18 02:23:54: DOWN for 3 minutes, 0 seconds
  01/07 14:59:11: DOWN for 1 minute, 0 seconds
HTTP Information for  https://uclouvain.be:443/probe.php
  Time to establish connection: 16 msecs
  Time spent connected to host: 134 msecs
Last updated Feb 08, 16:45:32; interval: 1 minute, 0 seconds
```

Data-centers

- Redundant connection to electrical grid
- UPS / diesel power generator
- Redundant servers / switches / connections
- Redundant power supplies
- Strict access-control
- Advanced fire protection
- Strict temperature and humidity conditions
- Dust control
- Disaster recovery plan

Data-centers layers

- Security layer (ACLs, network firewall, server firewall, application firewall)
- Load-balancing
- Application servers
- Load-balancing
- Database servers

Data-centers: load-balancer

- Shares the load between a pool of servers
- Servers can be removed or added to the pool on the fly
  - for maintenance purposes
  - due to an outage
  - to increase or decrease capacity
- Can provide SSL offloading

Data-centers: load-balancer

-Different load-spread techniques:

round robin

number of active connections

response time

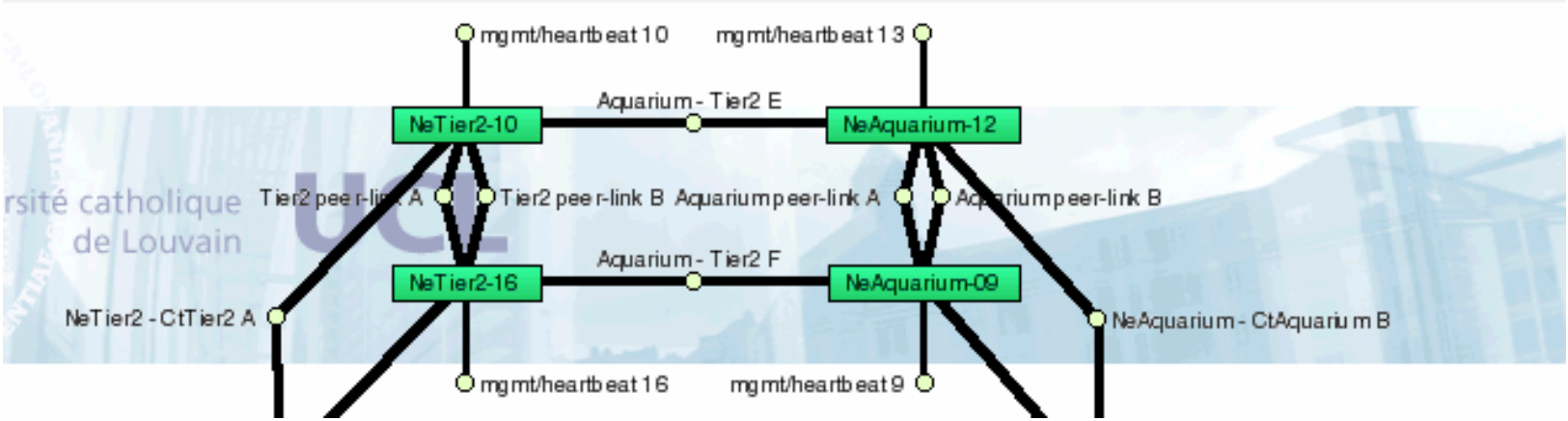
- Servers inside a pool are monitored using probes

ping

tcp connection

application call

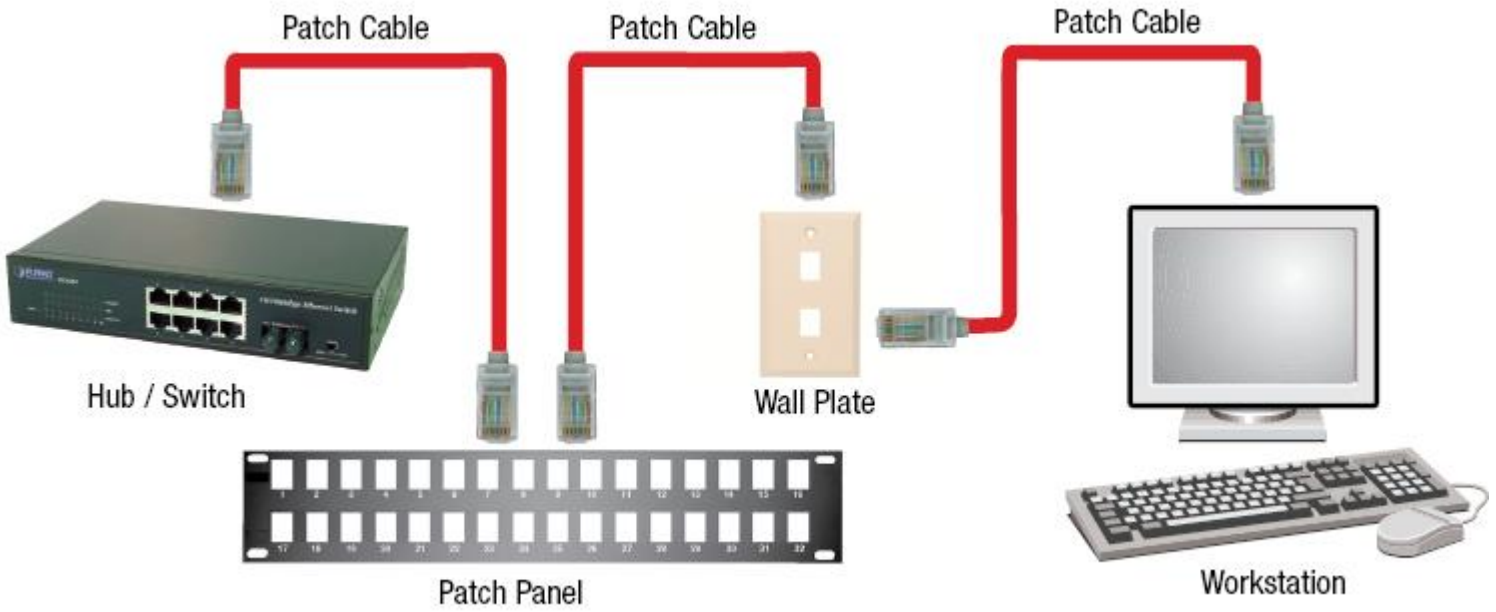
Data-centers



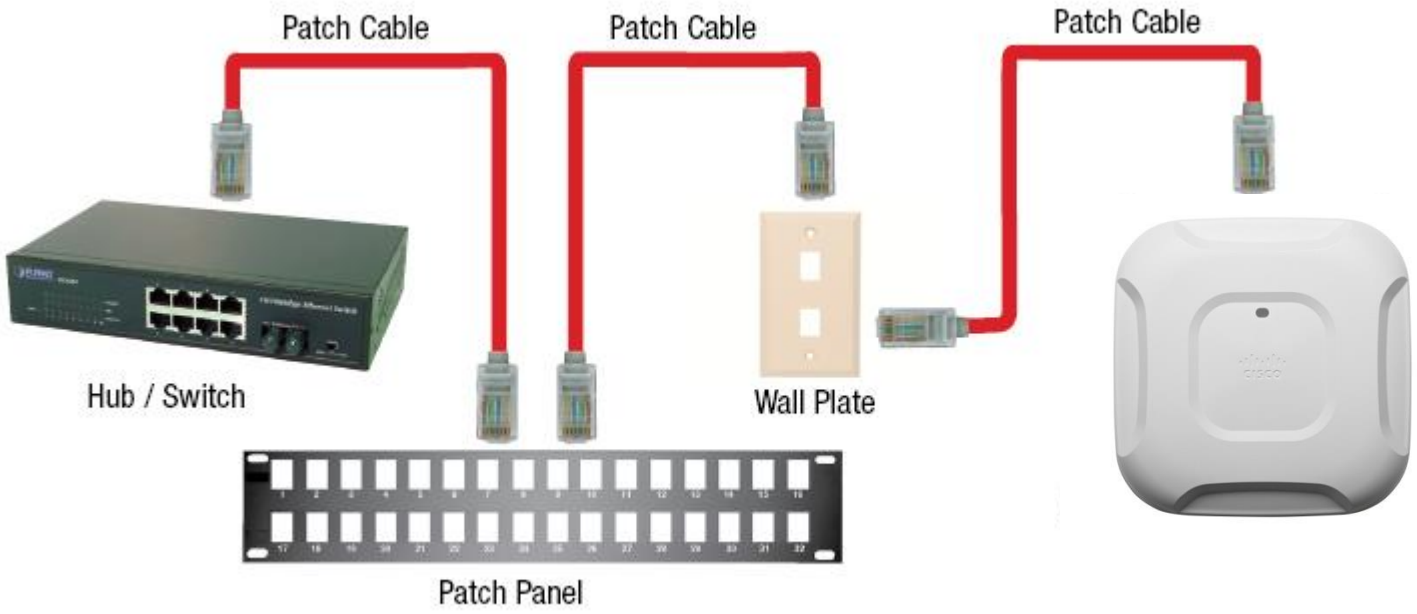
Campus

The wide part of UCL's network

Switches are located in patchrooms

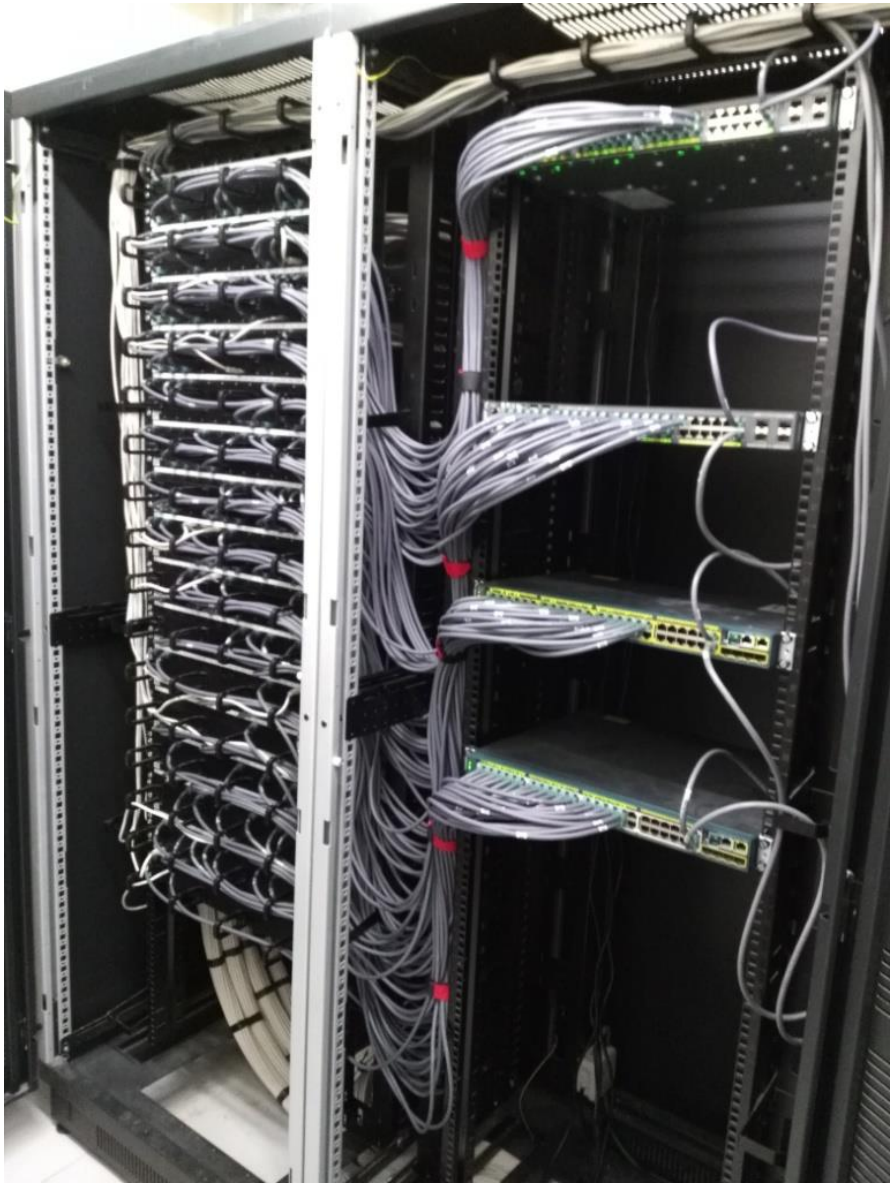


How patching is done



How patching is done

Example of a badly managed patchroom



properly managed patchroom

properly managed patchroom

Distribution and access layer

Each building is based on the same design

- 1 building switch:

  connected using fiber to the core network

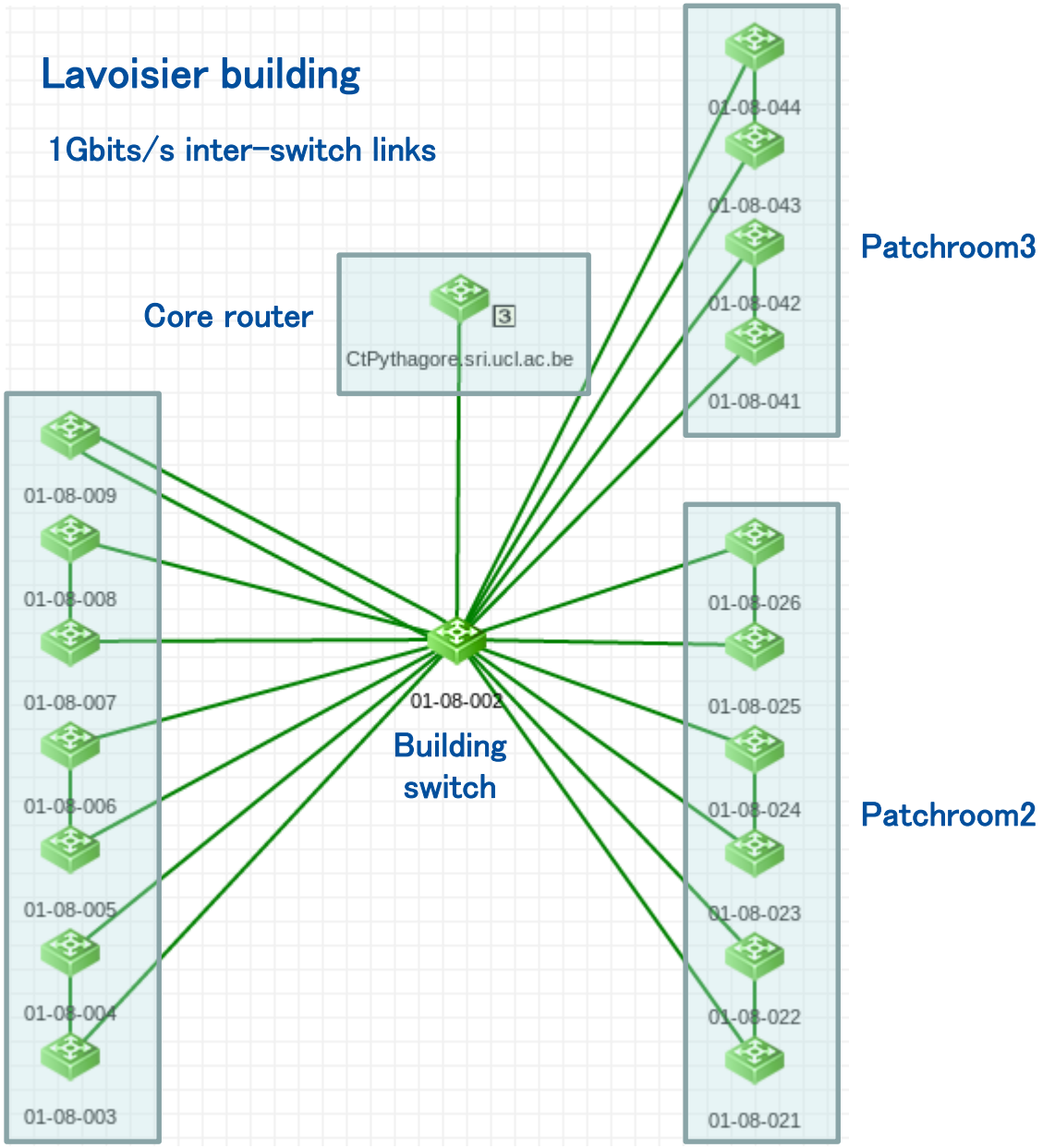
  connected using copper to access layer switches

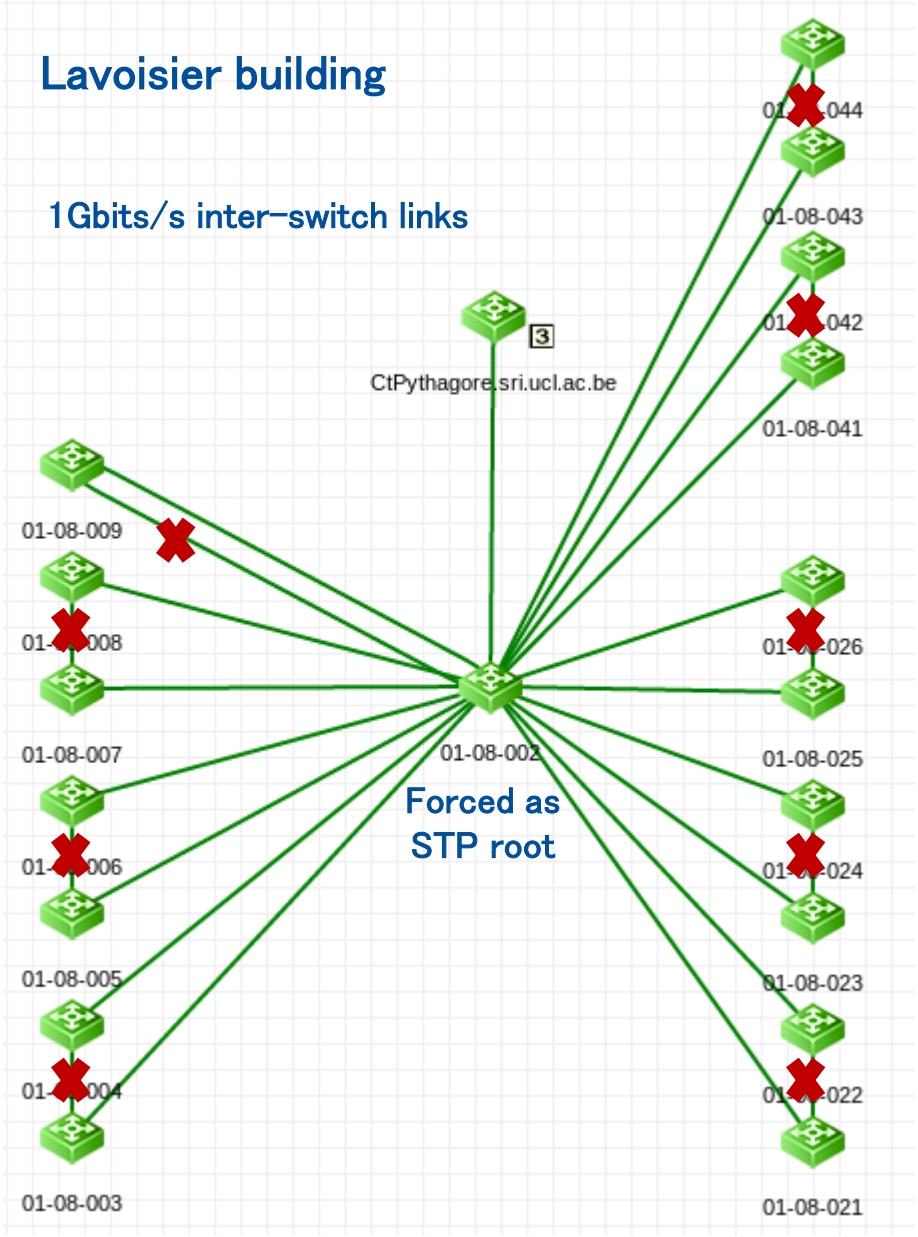
- Several access switches:

  hold device connections

- STP used to avoid loops at L2

- L3 routing done on core switch

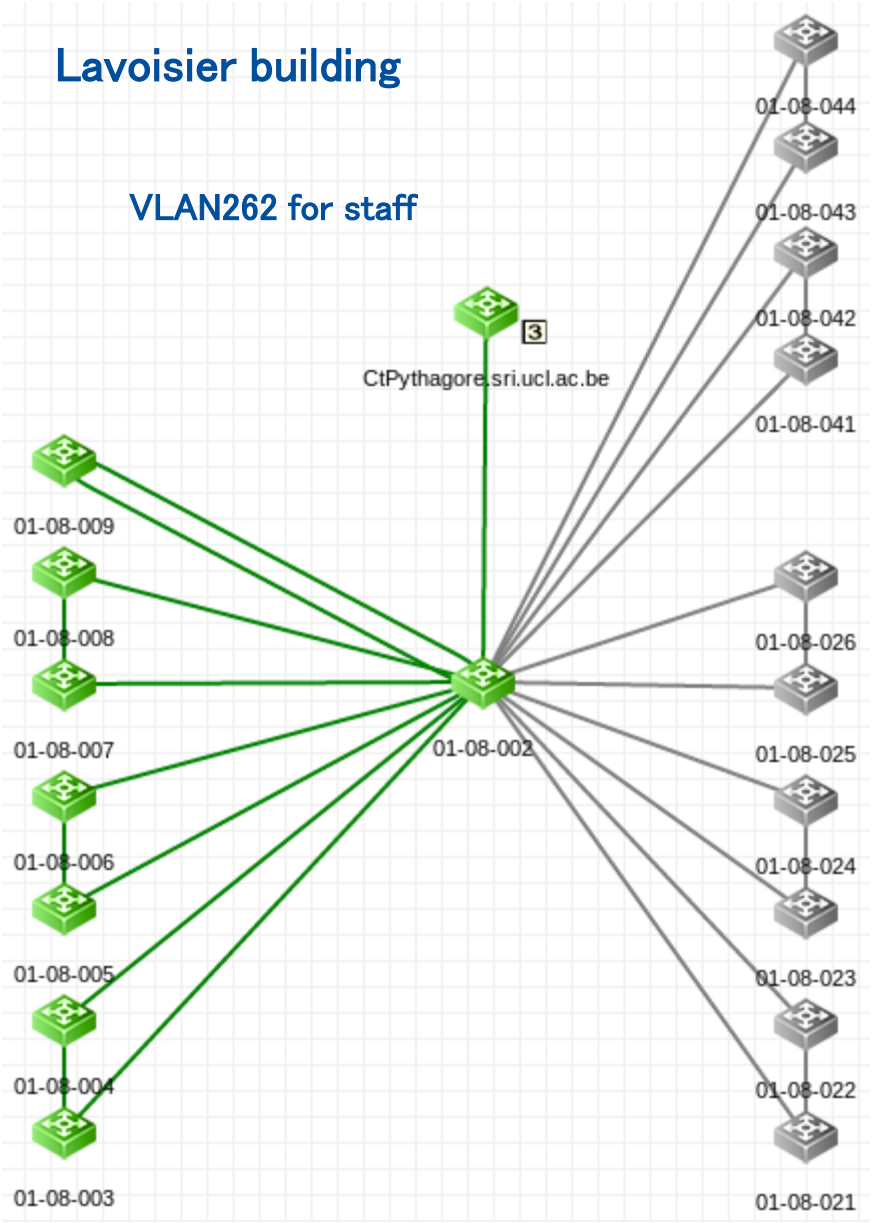

Lavoisier building
1Gbits/s inter-switch links
Core router
CtPythagore.sri.ucl.ac.be
3
Patchroom3
01-08-044
01-08-043
01-08-042
01-08-041
Patchroom1
01-08-009
01-08-008
01-08-007
01-08-006
01-08-005
01-08-004
01-08-003
01-08-002
Building switch
Patchroom2
01-08-026
01-08-025
01-08-024
01-08-023
01-08-022
01-08-021

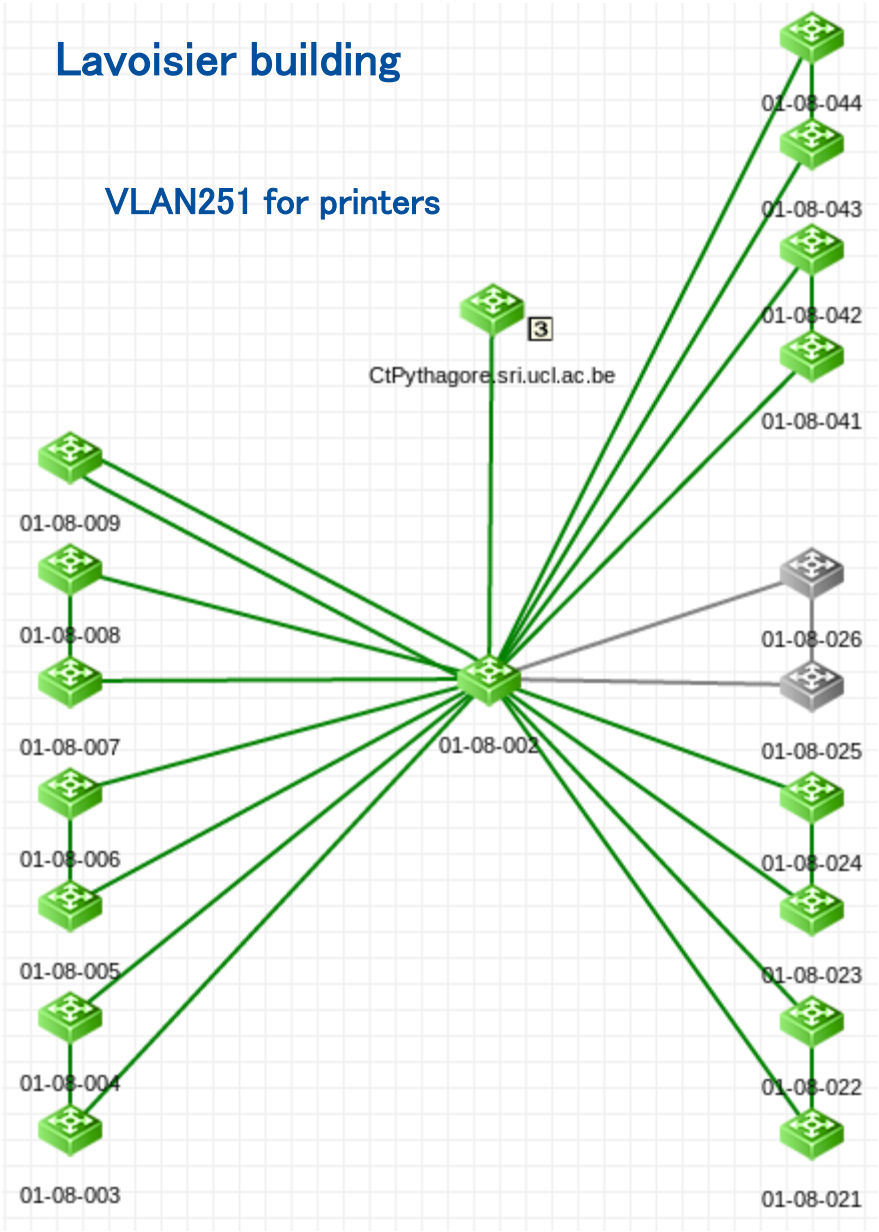

Lavoisier building
1Gbits/s inter-switch links
3
CtPythagore.sri.ucl.ac.be
01-08-044
01-08-043
01-08-042
01-08-041
01-08-009
01-08-008
01-08-007
01-08-006
01-08-005
01-08-004
01-08-003
01-08-002
Forced as
STP root
01-08-026
01-08-025
01-08-024
01-08-023
01-08-022
01-08-021

Distribution and access layer

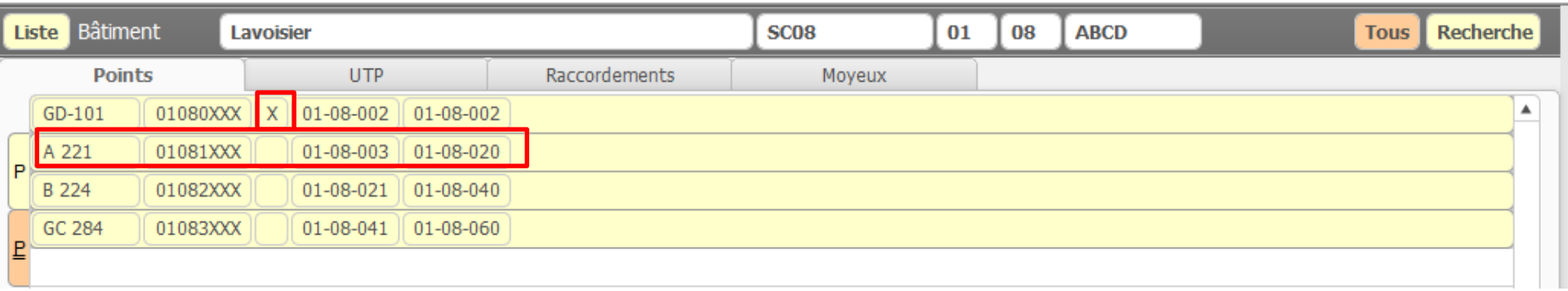
VLANs used to separate traffic from different groups at L2

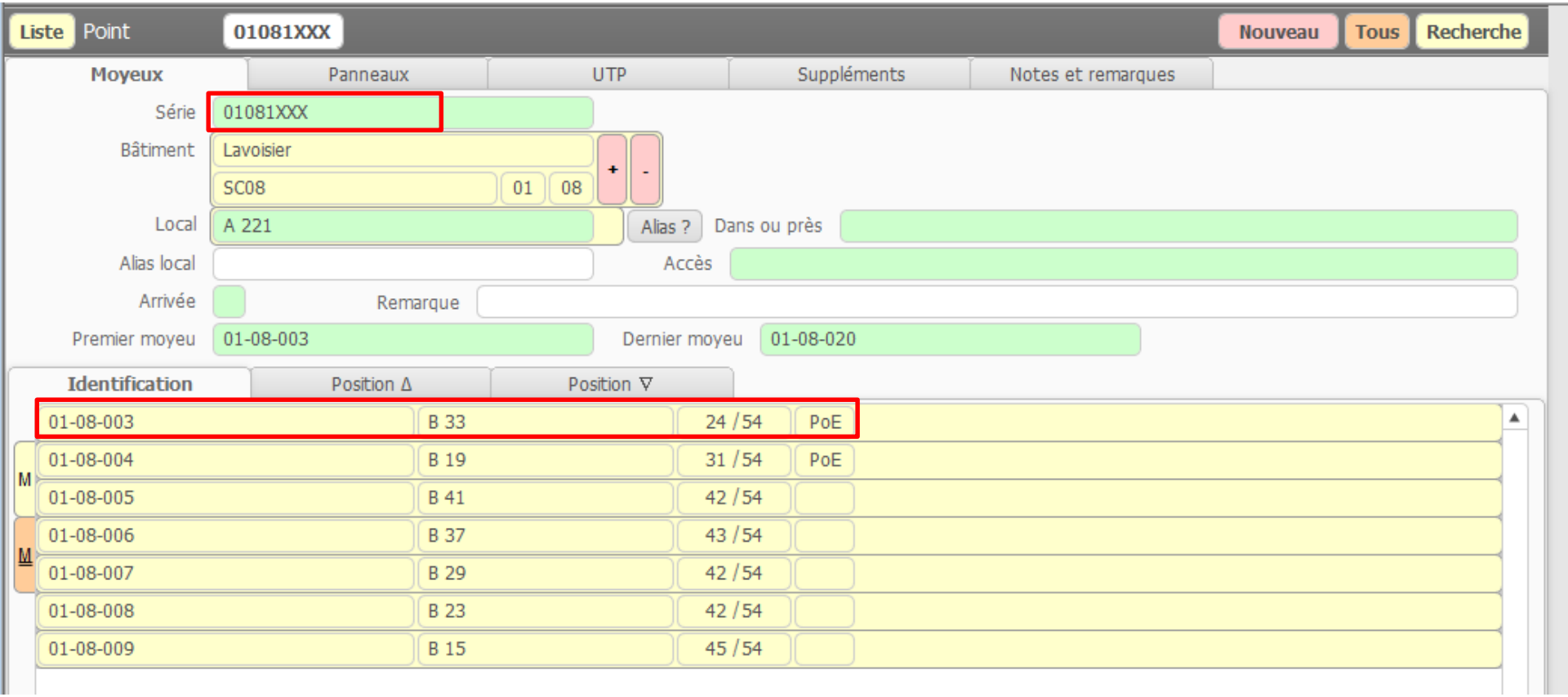
- Desktops used by students
- Desktops used by staff members
- Printers
- IP phones
- …

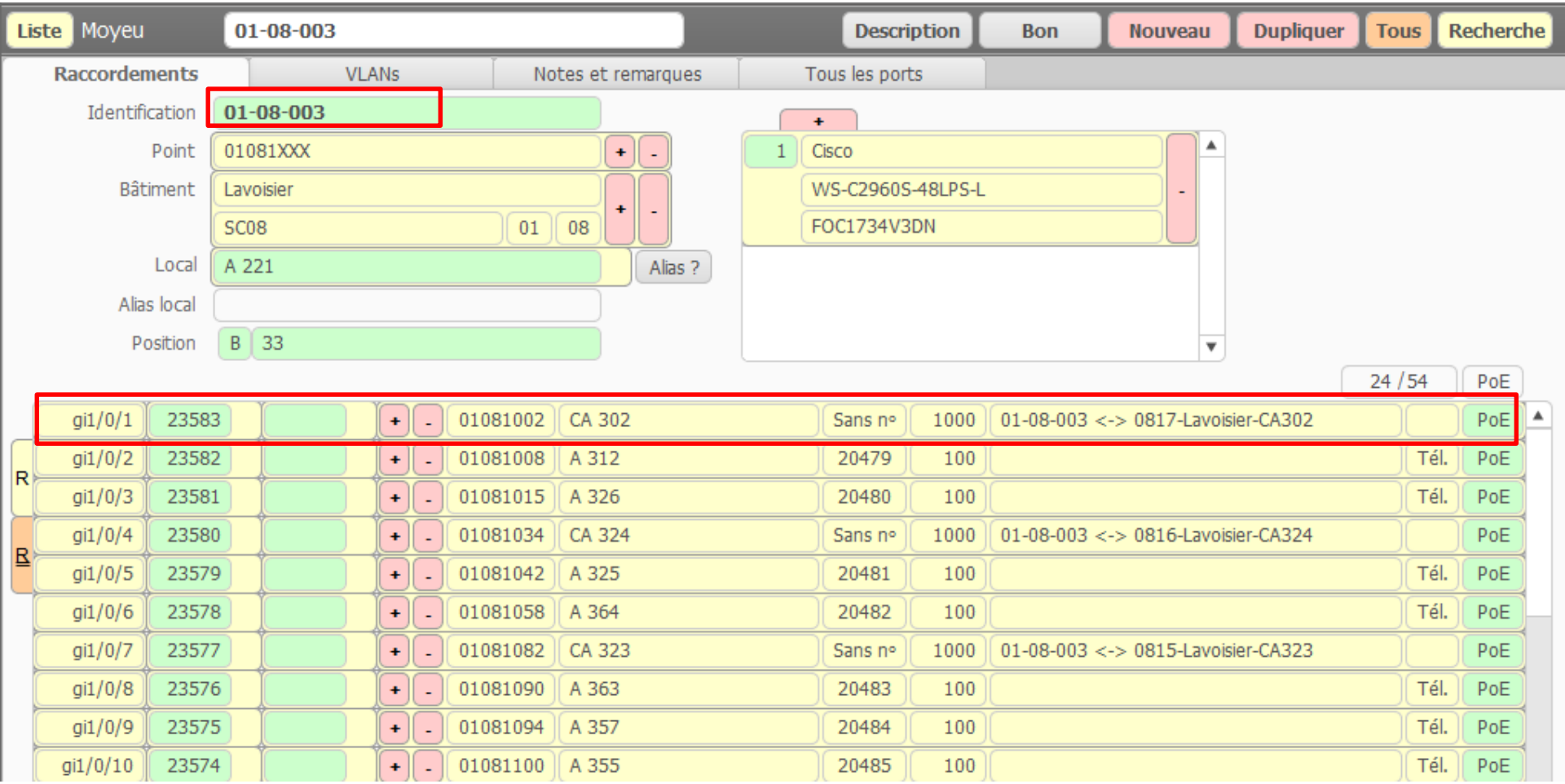

Lavoisier building
VLAN262 for staff
3
CtPythagore.sri.ucl.ac.be
01-08-002
01-08-044
01-08-043
01-08-042
01-08-041
01-08-009
01-08-008
01-08-007
01-08-006
01-08-005
01-08-004
01-08-003
01-08-026
01-08-025
01-08-024
01-08-023
01-08-022
01-08-021

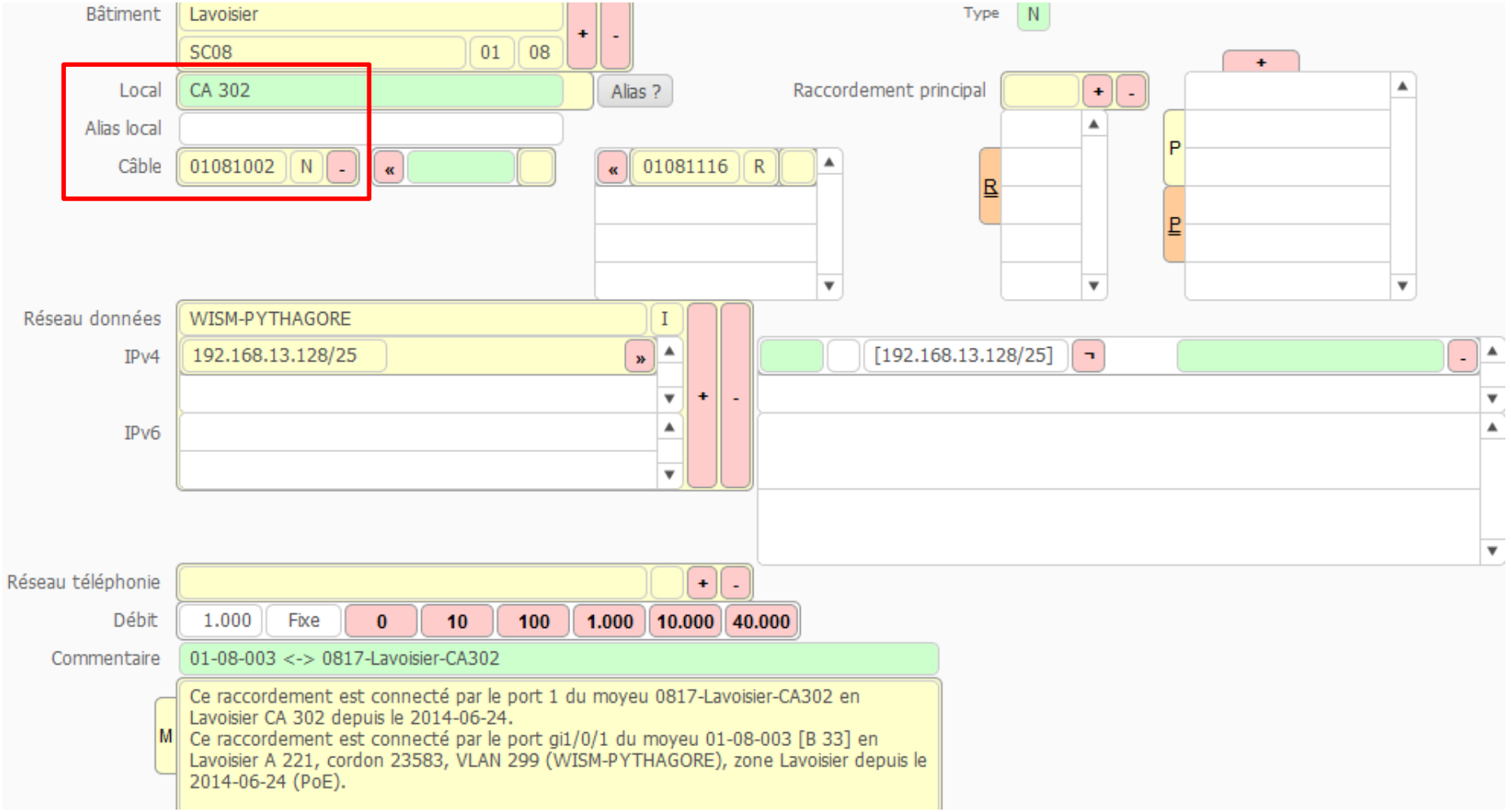

Lavoisier building
VLAN251 for printers
3
CtPythagore.sri.ucl.ac.be
01-08-044
01-08-043
01-08-042
01-08-041
01-08-009
01-08-008
01-08-007
01-08-006
01-08-005
01-08-004
01-08-003
01-08-002
01-08-026
01-08-025
01-08-024
01-08-023
01-08-022
01-08-021

Documentation is crucial




Liste
Point
01081XXX
Nouveau
Tous
Recherche
Moyeux
Panneaux
UTP
Suppléments
Notes et remarques
Série
01081XXX
Bâtiment
Lavoisier
SC08
01
08
+
-
Local
A 221
Alias ?
Dans ou près
Alias local
Accès
Arrivée
Remarque
Premier moyeu
01-08-003
Dernier moyeu
01-08-020
Identification
Position Δ
Position ∇
01-08-003 B 33 24 /54 PoE
01-08-004 B 19 31 /54 PoE
01-08-005 B 41 42 /54
01-08-006 B 37 43 /54
01-08-007 B 29 42 /54
01-08-008 B 23 42 /54
01-08-009 B 15 45 /54
M
M


Liste
Moyeu
01-08-003
Description
Bon
Nouveau
Dupliquer
Tous
Recherche
Raccordements
VLANs
Notes et remarques
Tous les ports
Identification
01-08-003
Point
01081XXX
Bâtiment
Lavoisier
SC08
01
08
Local
A 221
Alias ?
Alias local
Position
B
33
1
Cisco
WS-C2960S-48LPS-L
FOC1734V3DN
24 / 54
PoE
gi1/0/1 23583 01081002 CA 302 Sans n° 1000 01-08-003 <-> 0817-Lavoisier-CA302 PoE
gi1/0/2 23582 01081008 A 312 20479 100 Tél. PoE
gi1/0/3 23581 01081015 A 326 20480 100 Tél. PoE
gi1/0/4 23580 01081034 CA 324 Sans n° 1000 01-08-003 <-> 0816-Lavoisier-CA324 PoE
gi1/0/5 23579 01081042 A 325 20481 100 Tél. PoE
gi1/0/6 23578 01081058 A 364 20482 100 Tél. PoE
gi1/0/7 23577 01081082 CA 323 Sans n° 1000 01-08-003 <-> 0815-Lavoisier-CA323 PoE
gi1/0/8 23576 01081090 A 363 20483 100 Tél. PoE
gi1/0/9 23575 01081094 A 357 20484 100 Tél. PoE
gi1/0/10 23574 01081100 A 355 20485 100 Tél. PoE


Bâtiment
Lavoisier
SC08
01
08
Local
CA 302
Alias ?
Alias local
Câble
01081002
N
01081116
R
Type
N
Raccordement principal
R
P
P
Réseau données
WISM-PYTHAGORE
I
IPv4
192.168.13.128/25
[192.168.13.128/25]
IPv6
Réseau téléphonie
Débit
1.000
Fixe
0
10
100
1.000
10.000
40.000
Commentaire
01-08-003 <-> 0817-Lavoisier-CA302
M
Ce raccordement est connecté par le port 1 du moyeu 0817-Lavoisier-CA302 en Lavoisier CA 302 depuis le 2014-06-24.
Ce raccordement est connecté par le port gi1/0/1 du moyeu 01-08-003 [B 33] en Lavoisier A 221, cordon 23583, VLAN 299 (WISM-PYTHAGORE), zone Lavoisier depuis le 2014-06-24 (PoE).

QoS

- Prioritization needed because of the wide range of devices and applications using the network
- Different RTT, jitter and bandwidth constraints
- Kicks in only when congestion occurs
- Packets are tagged with a priority
- Voice calls get the highest priority but at low bandwidth
- Security cameras flows get higher priority
- Other flows get normal priority
- Access ports with more than 50Mbit/s traffic get low priority

Security considerations

- Enforce security rules as close as possible to the source.
- Switches inspect user traffic to:
  - drop unauthorized router advertisements (RA)
  - deny unauthorized DHCP servers
  - allow traffic only if DHCP transaction completed
  - avoid address spoofing
- Routers check if source IP correspond to the defined network
- ACLs / firewalls are present on specific networks

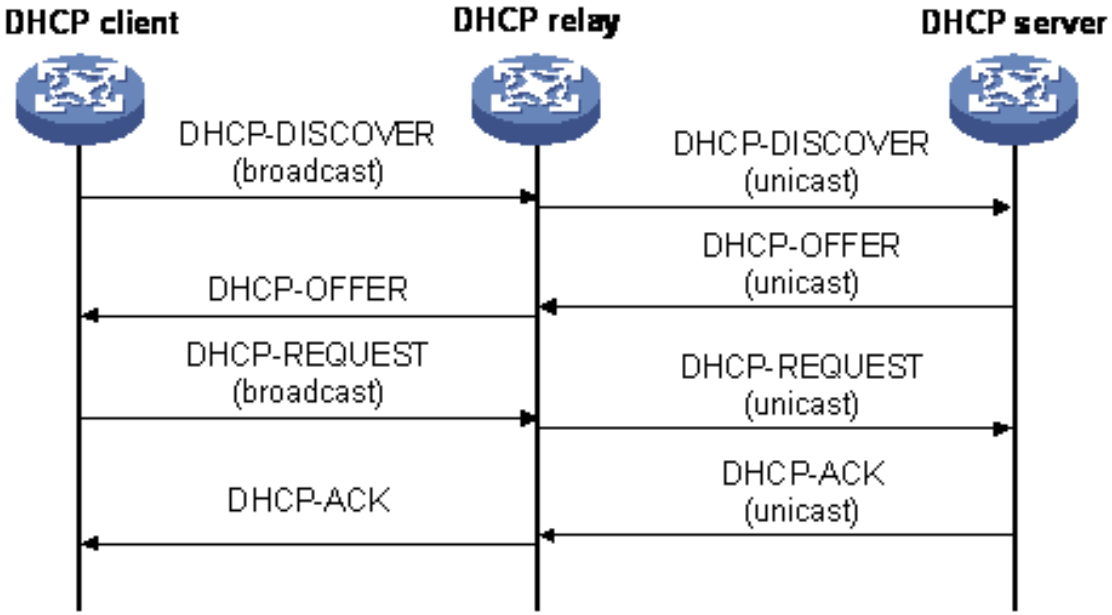
```
01-16-012#sh ipv6 neighbors binding
Binding Table has 79 entries, 79 dynamic
Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DHCP, PKT - Other Packet, API - API created

    IPv6 address                     Link-Layer addr Interface vlan prlvl  age   state    Time left
ND  FE80::FAB1:56FF:FECB:10A5        F8B1.56CB.10A5  Gi1/0/2    238  0005    4mn REACHABLE  24 s try 0
ND  2001:6A8:3081:4160:F803:99A6:37CA:53DF  E8EA.6A00.159B  Gi1/0/38   225  0005  237mn STALE      73544 s
```

Address assignment

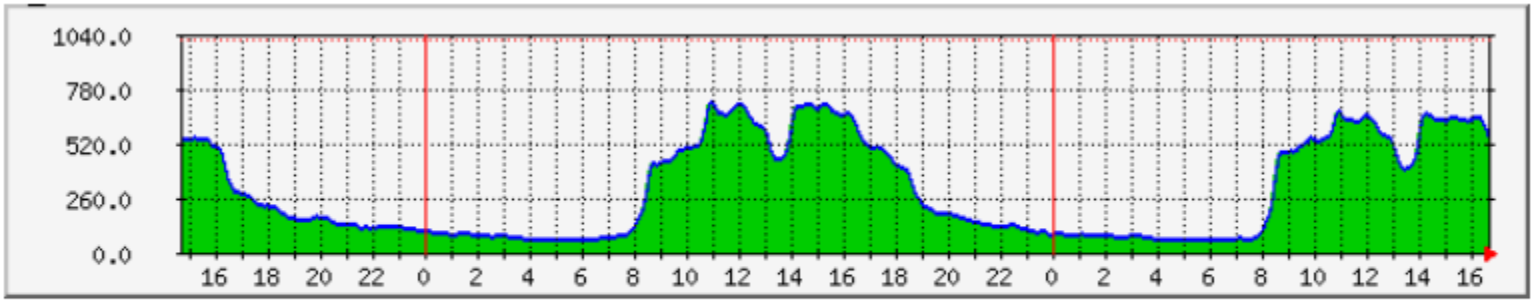
- Avoid manually assigned addresses:
  - generates a lot of configuration burden
  - prone to human error
- Unable to dynamically renumber a network
- Exceptions exist for network devices and specific servers

DHCP

- One global redundant DHCP infrastructure hosted in the DC
- Routers act as a DHCP relay agent



DHCP monitoring



	Max	Moyenne	Actuel
Adr. IP utilises:	712 adresse(s)	291 adresse(s)	538 adresse(s)

Number of distributed IPs on a DHCP pool used for WiFi

DNS

LLN DC1

NS1

LLN DC2

NS2

Woluwe

NS3

Belnet

NS1

NS2

```
-qhunin@vps73519:~$ dig @130.104.1.1 uclouvain.be NS
-(…)
-;; QUESTION SECTION:
-;uclouvain.be.                         IN      NS

-;; ANSWER SECTION:
-uclouvain.be.          604800  IN      NS      ns3.sri.ucl.ac.be.
-uclouvain.be.          604800  IN      NS      ns2.belnet.be.
-uclouvain.be.          604800  IN      NS      ns1.sri.ucl.ac.be.
-uclouvain.be.          604800  IN      NS      ns2.sri.ucl.ac.be.
-uclouvain.be.          604800  IN      NS      ns1.belnet.be.
-;; ADDITIONAL SECTION:
-ns1.sri.ucl.ac.be.     604800  IN      A       130.104.1.1
-ns2.sri.ucl.ac.be.     604800  IN      A       130.104.1.2
-ns3.sri.ucl.ac.be.     604800  IN      A       130.104.254.1
-ns1.sri.ucl.ac.be.     604800  IN      AAAA    2001:6a8:3081:1::53
-ns2.sri.ucl.ac.be.     604800  IN      AAAA    2001:6a8:3081:2::53
-ns3.sri.ucl.ac.be.     604800  IN      AAAA    2001:6a8:3082:1::53
```

DNS

- Two different views:

one for the external world

DNS servers respond only for UCL's domains

one for the internal network

DNS servers respond for all domains

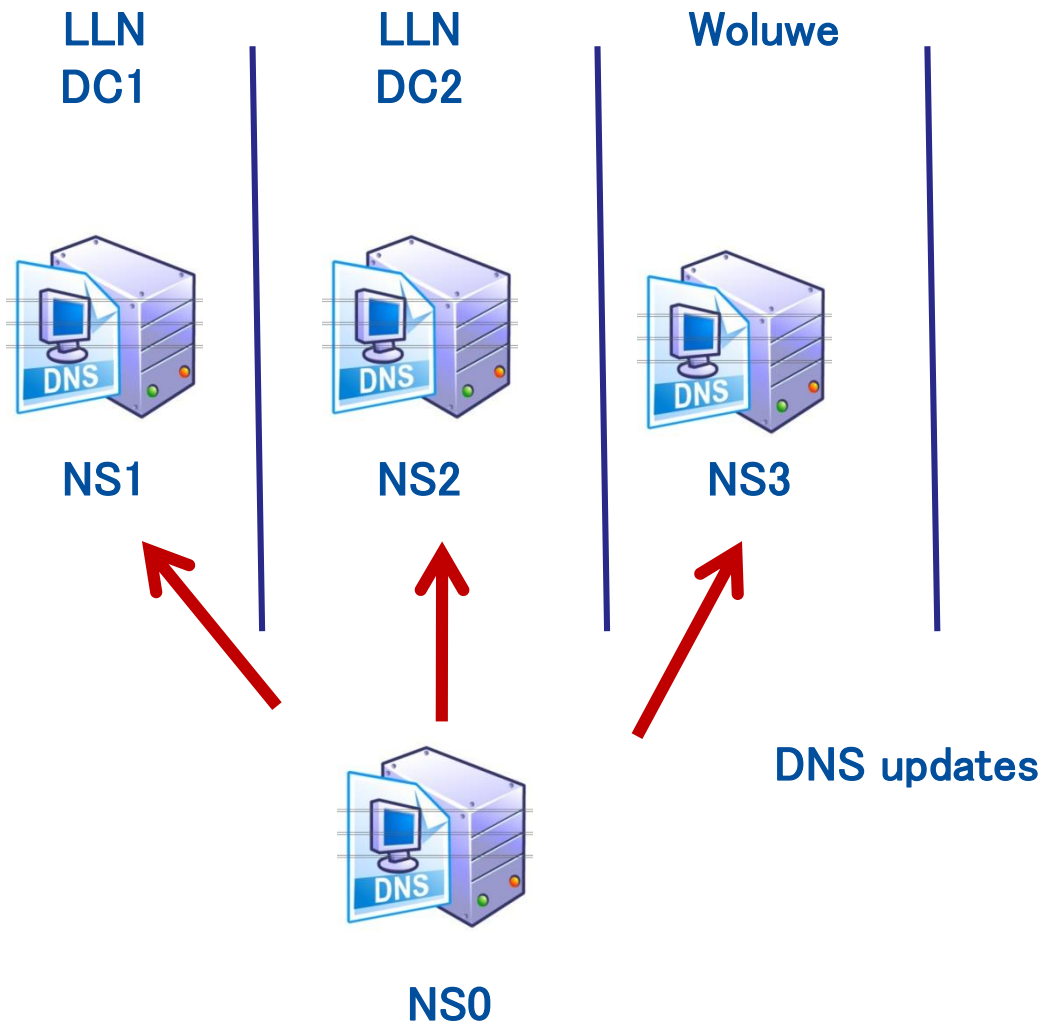
recursive DNS

DNS – security

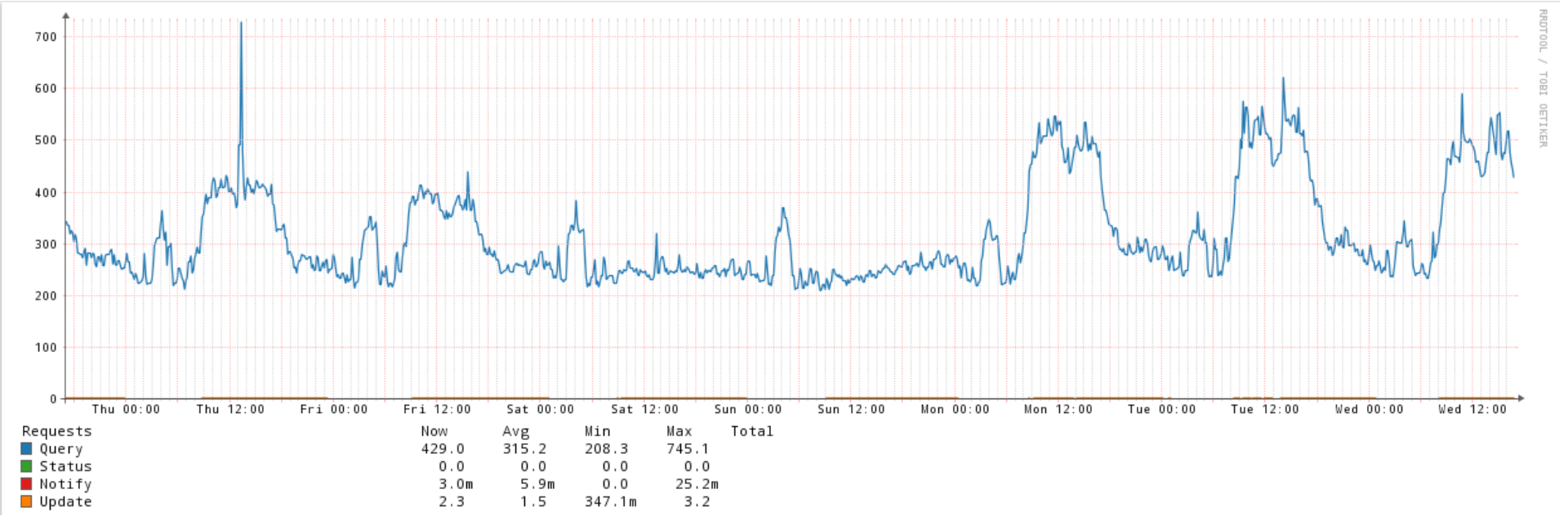
- DNSSec: DNS responses are signed using cryptography

- Hidden master: holds the authoritative DB

  does not serve client queries


LLN
DC1
LLN
DC2
Woluwe
DNS
DNS
DNS
NS1
NS2
NS3
DNS updates
DNS
NS0

DNS monitoring



Nbr of incoming DNS requests per second on NS1

Monitoring tools

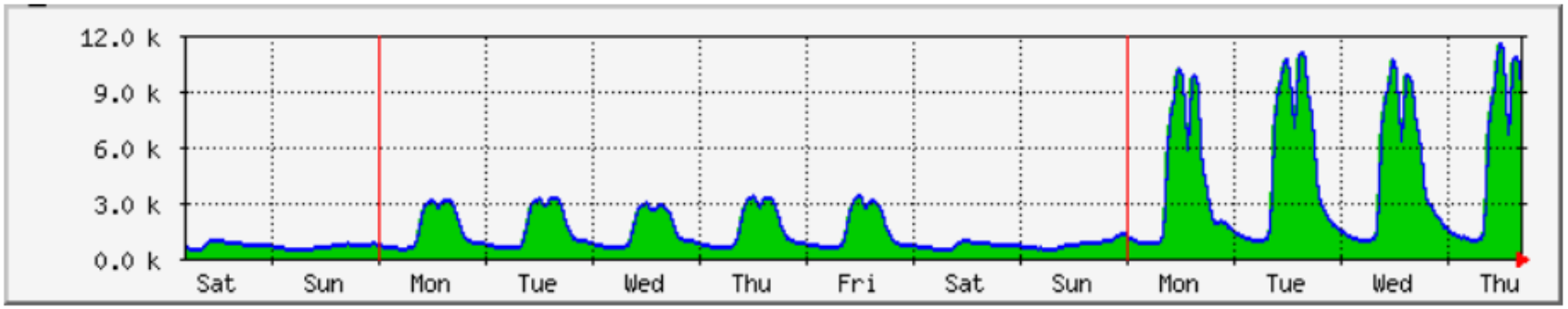
- Essential to see, detect and understand
  - what happened
  - what's happening
  - what will happen
- Used for proactive and reactive action during:
  - incidents
  - capacity planning
  - design
- Uses SNMP, netflows, syslog and/or CLI to collect data

Management tools

- Essential to be able to scale
- Examples:
  - configuration backup automation
  - software update automation
  - automated configuration deployment
  - …

Monitoring

Graphique hebdomadaire (sur 30 minutes : Moyenne)

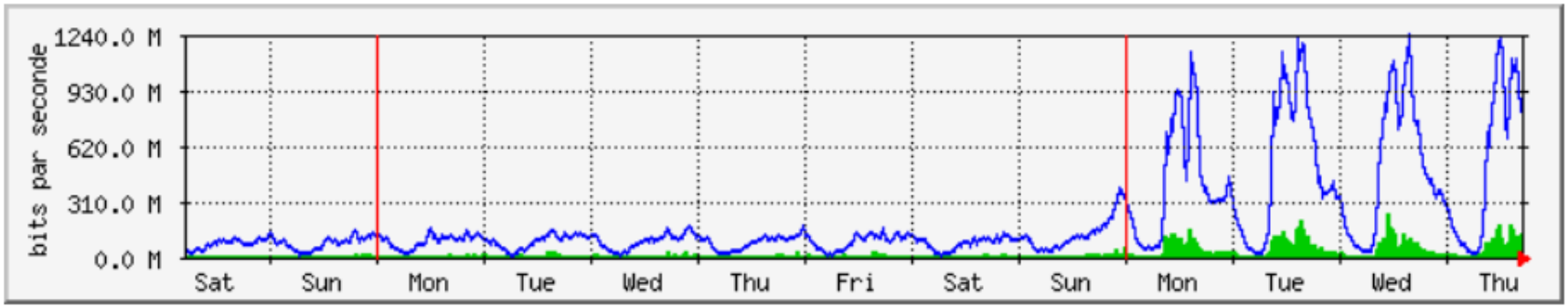


	Max	Moyenne	Actuel
Clients:	11 kClients	2113 Clients	8866 Clients
Sortie	11 kClients	2113 Clients	8866 Clients

Total number of simultaneous WiFi clients

Monitoring

Graphique hebdomadaire (sur 30 minutes : Moyenne)

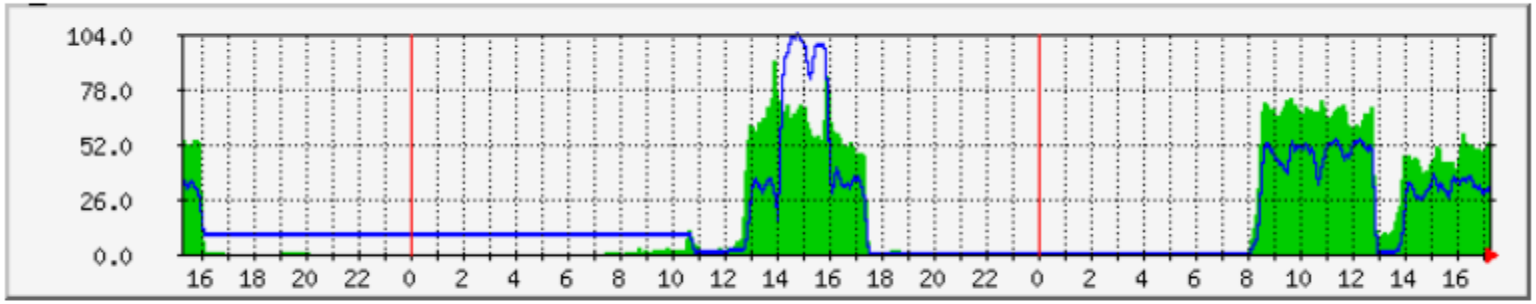


	Max	Moyenne	Actuel
Entrée	242.8 Mb/s (2.4%)	20.3 Mb/s (0.2%)	131.9 Mb/s (1.3%)
Sortie	1229.3 Mb/s (12.3%)	198.8 Mb/s (2.0%)	850.1 Mb/s (8.5%)

Student's bandwidth usage on WiFi

Monitoring

Graphique quotidien (sur 5 minutes : Moyenne)

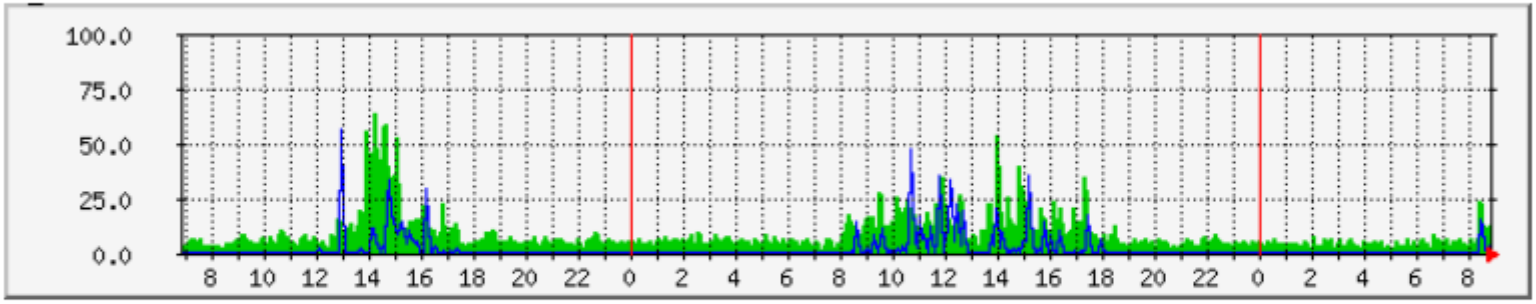


	Max	Moyenne	Actuel
2.4Ghz:	91 Clients	20 Clients	53 Clients
5Ghz:	104 Clients	19 Clients	32 Clients

Number of connected clients on one of the WiFi access points in the SC10 auditorium

Monitoring

Graphique quotidien (sur 5 minutes : Moyenne)



	Max	Moyenne	Actuel
2.4Ghz:	64 %	9 %	13 %
5Ghz:	55 %	2 %	1 %

Medium usage on one of the WiFi access points
in the SC10 auditorium

WiFi is slow

-Is it due to:

- user's computer
- a coverage issue
- interference issue
- saturated WiFi access point
- saturated uplink on the wired part
- WiFi controller issue
- limit of available commercial bandwidth reached
- service provider issue
- destination website issue
- …

The future

Core network replacement

Vision : provide a secure and seamless mobility experience to users throughout the campus no matter if they are connected using WiFi or wired, onsite or remotely.

The future

- Increase bandwidth capacity
- Provide network services as an Enterprise Service Provider
- Ability to virtually segment the network
- Reduce configuration tasks
- Increase flexibility
- Reduce lead time
- Use automation

UCL Université catholique de Louvain

Infrastructures de production du système d'information (SIPR)
Service Général du Système d'Information (SGSI)

UCL

Université
catholique
de Louvain