Campus IPv6 connection – Campus IPv6 deployment

Campus Address allocation, Topology Issues

János Mohácsi

NIIF/HUNGARNET

Copy …Rights

- *This slide set is the ownership of the 6DISS project via its partners*
- *The Powerpoint version of this material may be reused and modified only with written authorization*
- *Using part of this material must mention 6DISS courtesy*
- *PDF files are available from www.6diss.org*

Contributions

- Main authors
  - János Mohácsi, NIIF/HUNGARNET - Hungary
- Contributors
  - Jérôme Durand, Renater, France
  - Tim Chown, University of Southampton, Great-Brittain

Various Campus transition approaches

- Tunneling (“connecting IPv6 clouds”)
  – IPv6 packet is data payload of IPv4 packet/or MPLS frames
- Translation methods (“IPv4<->IPv6 services”)
  – Layer 3: Rewriting IP header information (NAT-PT)
  – Layer 4: Rewriting TCP headers
  – Layer 7: Application layer gateways (ALGs)
- Dual Stack
  – Servers/clients speaking both protocols
  – Application/service can select either protocol to use

Benefits of dual-stack deployment

- By deploying dual-stack, you can test IPv6-only devices/services without disrupting IPv4 connectivity
- Dual stack IPv6 + IPv4 NAT: legacy IPv4 applications (email, www) can be used next to new IPv6 applications (p2p, home networking, …)
  - IPv6 offers the next generation of applications

Campus deployment plan /1

- Obtain global IPv6 address space from your ISP
  - NRENs usually has a /32 prefix from RIPE NCC/RIRs
  - A university will get a /48 prefix from NRENs
- Obtain external connectivity
  - You can do dual-stack connectivity
  - Many universities will use tunnel to to get IPv6 service
    - in this case be sure that nobody can abuse your tunnel – use filtering

Campus deployment plan /2

- Internal deployment
  - Determine an IPv6 firewall/security policy
  - Develop an IPv6 address plan for your site
  - Determine address management policy (RA/DHCPv6?)
  - Migrate to dual-stack infrastructure on the wire
    - Network links become IPv6 enabled
  - Enable IPv6 on host systems (Linux, WinXP, …)
  - Enable IPv6 services and applications
    - Starting with DNS
  - Enable management and monitoring tools

Campus Addressing

- Most sites will receive /48 assignments:

Network address (48 bits)	16bits	EUI host address (64 bits)

- 16 bits left for subnetting - what to do with them?

Campus Addressing

- Sequentially, e.g.
  - 0000
  - 0001
  - …
  - FFFF

  - 16 bits = 65535 subnets

Campus Addressing

- 2. Following existing IPv4:
  - Subnets or combinations of nets & subnets, or VLANs, etc., e.g.
  - 152.66.**60**.0/24 .003c
  - 152.66.**91**.0/24 .005b
  - 152.66.**156**.0/24 .009c

Campus Addressing

- Topological/aggregating
- reflecting wiring plants, supernets, large broadcast domains, etc.
  - Main library = 0010/60
    - Floor in library = 001a/64
  - Computing center = 0200/56
    - Student servers = 02c0/64
  - Medical school = c000/52
  - and so on. . .

New Things to Think About

- You can use “all 0s” and “all 1s”! (0000, ffff)
- You’re not limited to 254 hosts per subnet!
  - Switch-rich LANs allow for larger broadcast domains (with tiny collision domains), perhaps thousands of hosts/LAN…
- No “secondary subnets” (though >1 address/interface)
- No tiny subnets either (no /30, /31, /32)—plan for what you need for backbone blocks, loopbacks, etc.
- You should use /64 per links!

New Things to Think About

- Every /64 subnet has far more than enough addresses to contain all of the computers on the planet, and with a /48 you have 65536 of those subnets - use this power wisely!
- With so many subnets your IGP may end up carrying thousands of routes - consider internal topology and aggregation to avoid future problems.

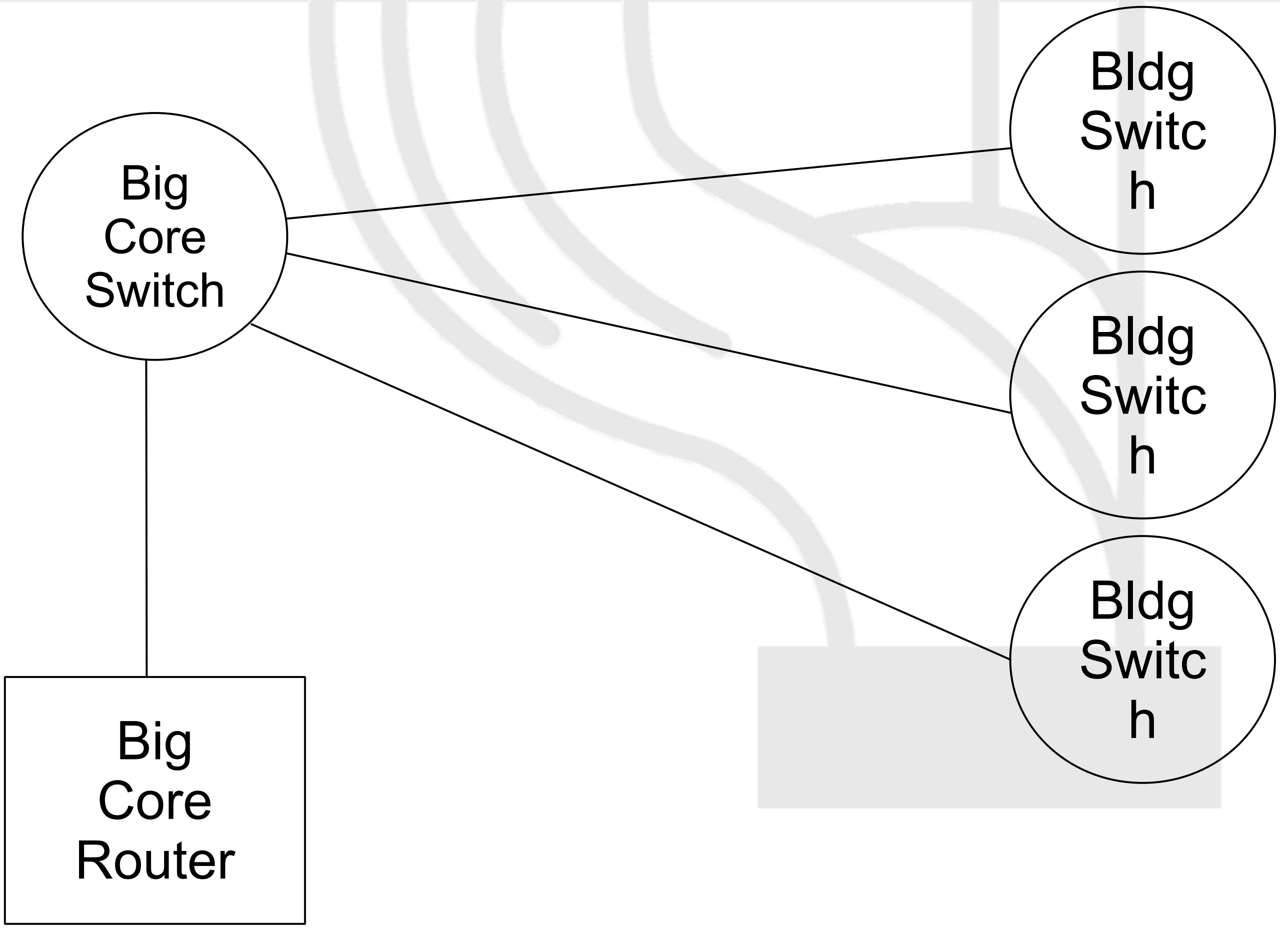
New Things to Think About

- Renumbering will likely be a fact of life. Although v6 does make it easier, it still isn't pretty. . .
  - Avoid using numeric addresses at all costs
  - Avoid hard-configured addresses on hosts except for servers (this is very important for DNS servers) – use the feature that you can assign more than one IPv6 address to an interface (IPv6 alias address for servers)
  - Anticipate that changing ISPs will mean renumbering

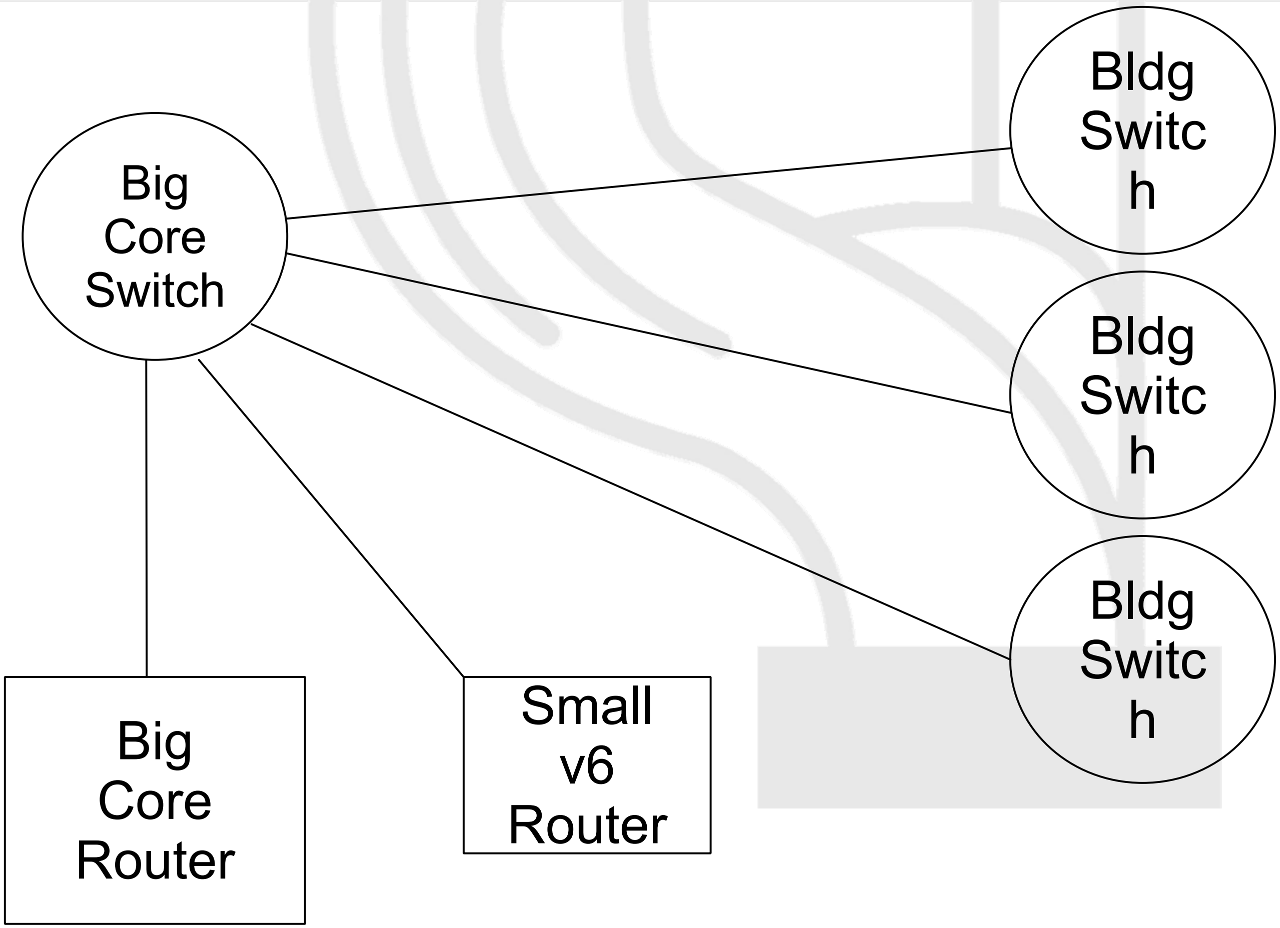
Topology Issues

V6 in a production network

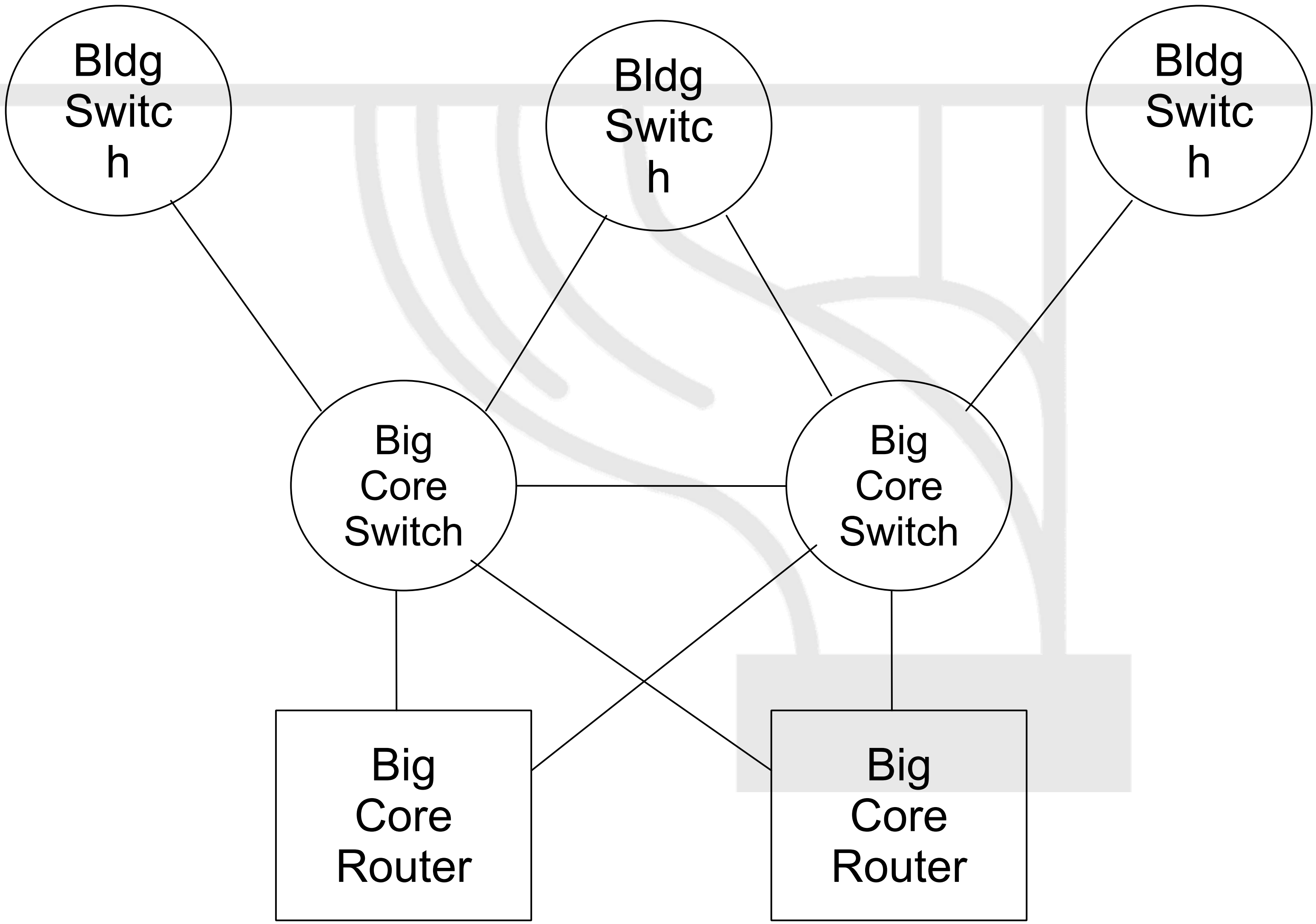
Layer-2 Campus -1 Switch



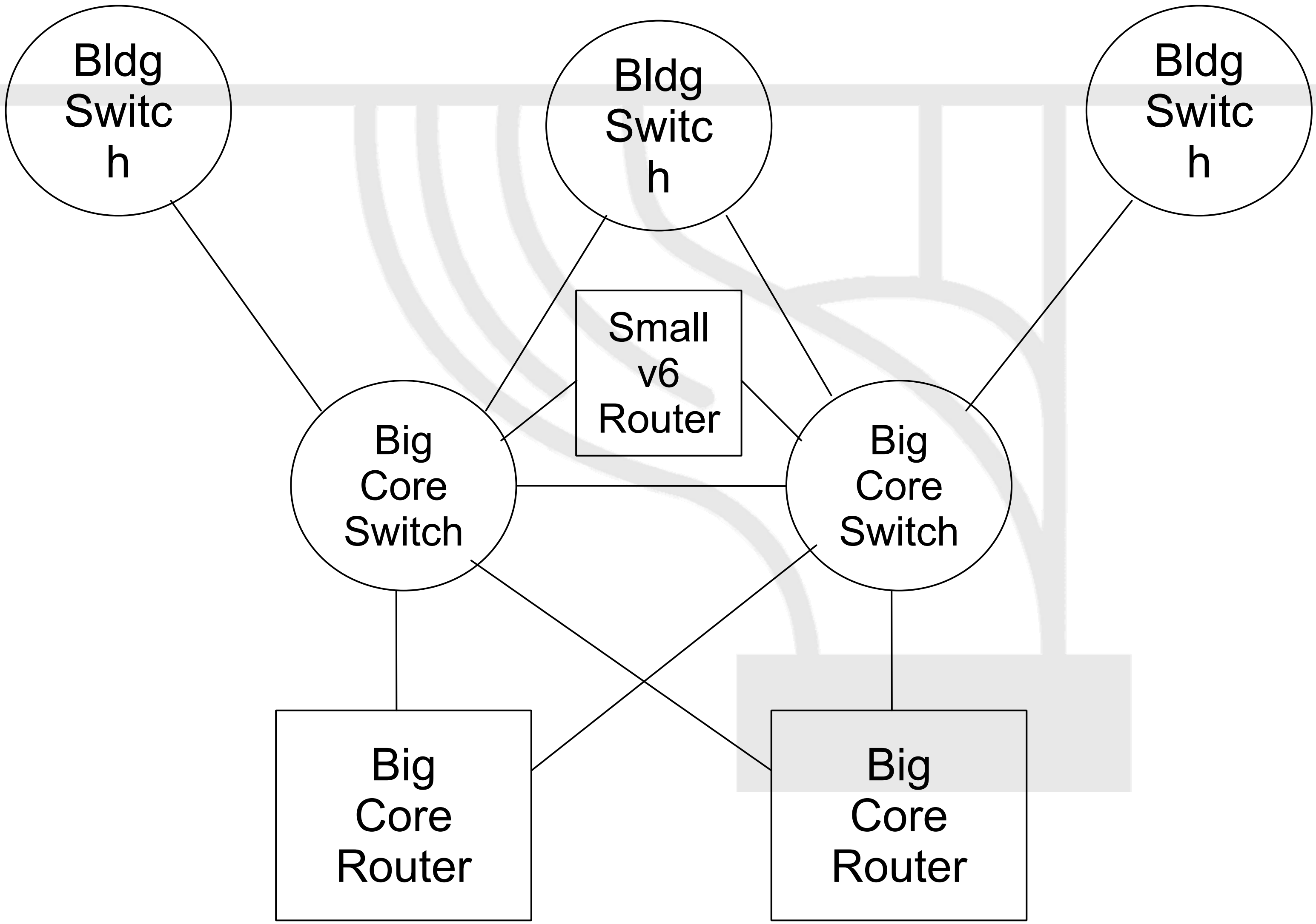
Layer-2 Campus - 1 Switch



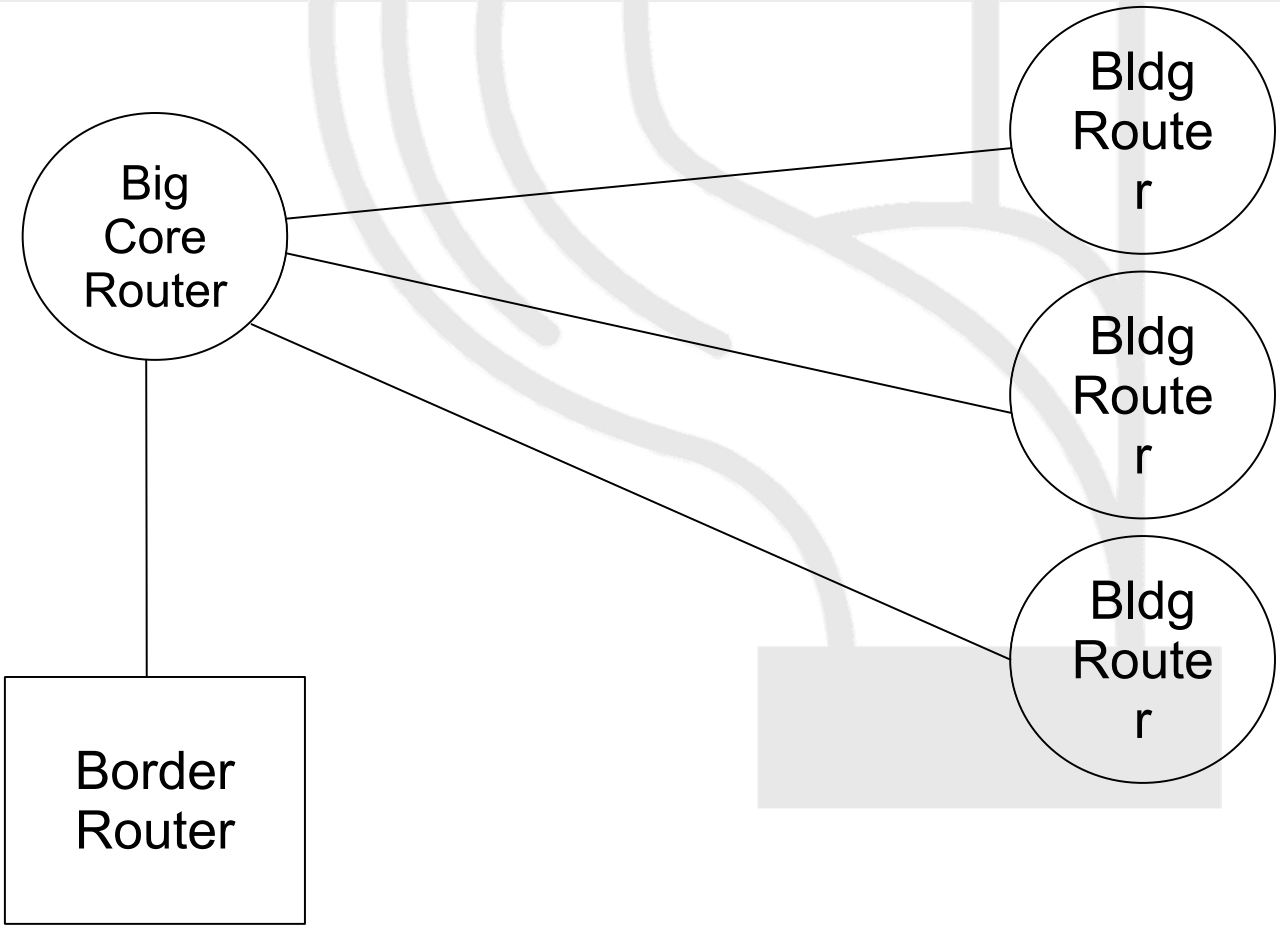
Layer-2 Campus - Redundant Switches



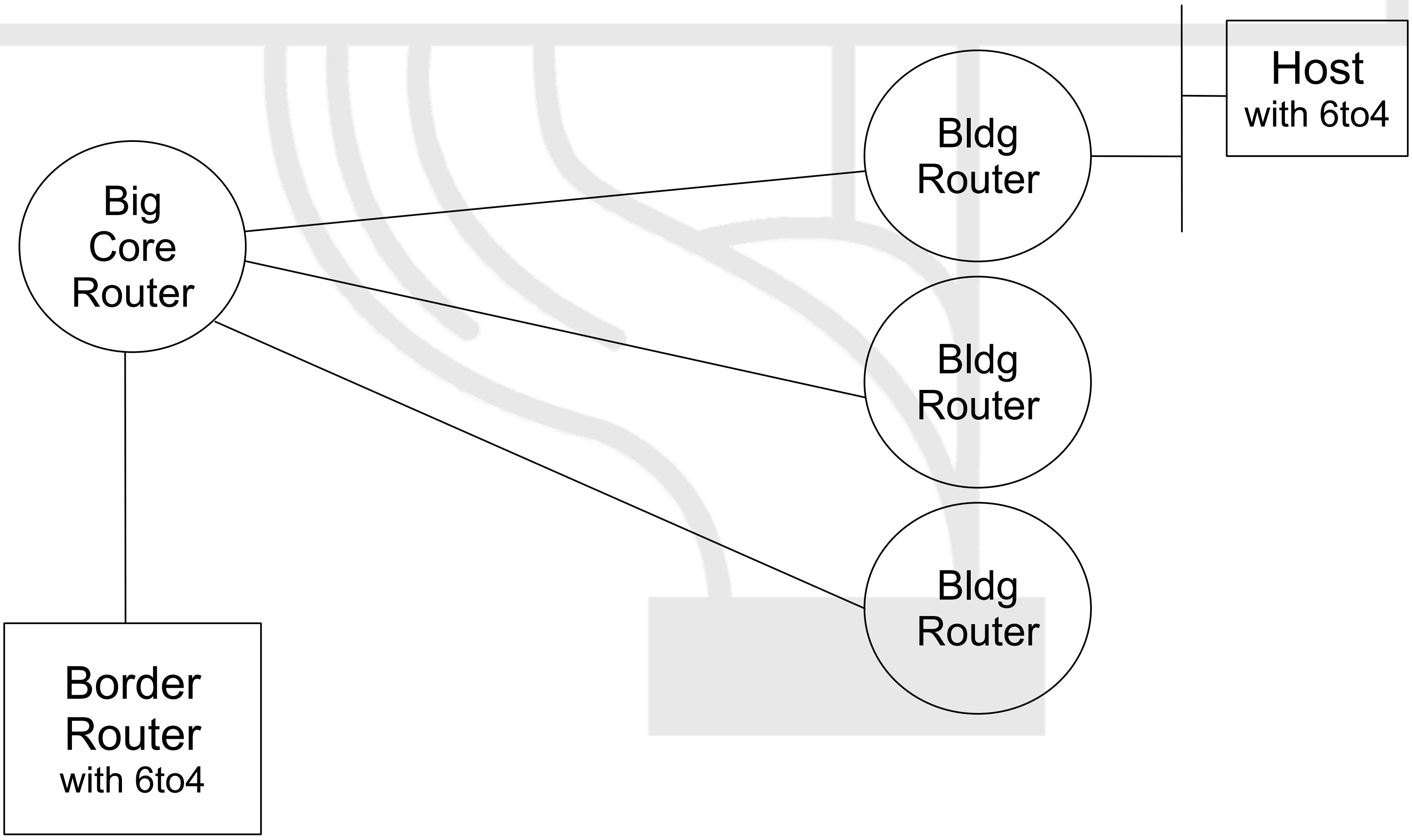
Layer-2 Campus Redundant Switches



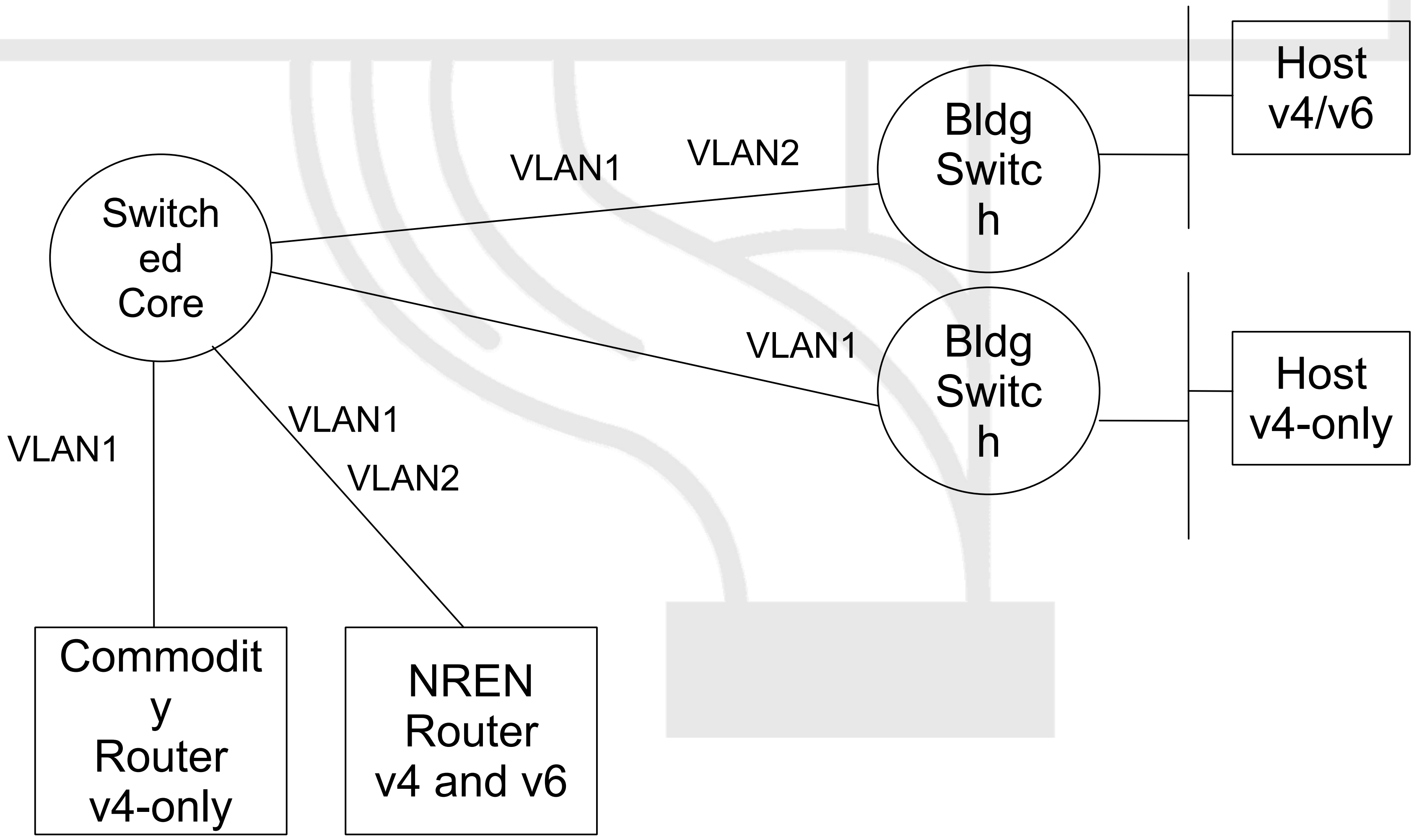
Layer-3 Campus



Layer-3 Campus



Edge Router Options



Routing Protocols

- iBGP and IGP (IS-IS/OSPFv3)
  - IPv6 iBGP sessions in parallel with IPv4
  - You need IPv4 router-id for IPv6 BGP peering
- Static Routing
  - all the obvious scaling problems, but works OK to get started, especially using a trunked v6 VLAN.
- OSPFv3 is might be good
  - It will run in a ships-in-the-night mode relative to OSPFv2 for IPV4 - neither will know about the other.

Management and monitoring

- Device configuration and monitoring - SNMP
- Statistical monitoring e.g. Cricket/MRTG
- Service monitoring - Nagios
- Intrusion detection (IDS)
- Authentication systems
  - For example, 802.1x + RADIUS for WLAN
- See more later

How to enable IPv6 services?

- Add v6 testing service for different name first:
  - service.v6.fqdn or service6.fqdn with AAAA + reverse PTR entry.
  - Test it
- Add v6 service under the same name:
  - service.fqdn with A +AAAA and two PTR.

How to enable IPv6 services if you don’t have IPv6 capable server?

- Use proxy (more exactly reverse-proxy) server
  - Apache2 proxy is a very good one
- Use netcat
  - Kind of hack ☺

Apache2 reverse proxy

- Configuration is very easy:

```
ProxyRequests Off
ProxyPass / http://ipv4address
ProxyPassReverse /
  http://ipv4address
ProxyPreserveHost On
```

Reverse proxy advantages & disadvantages

- Advantage:
  - Fast implementation, instantly provide web service over IPv6
  - No modifications required in a production web server environment
  - Allow for timely upgrading of systems
  - Scalable mechanism: a central proxy can support many web sites
- Disadvantage:
  - Significant administrative overhead for large scale deployment
  - May break advanced authentication and access control schemes
  - Breaks statistics: all IPv6 requests seem to be coming from the same address (may be fixed with filtering and concatenation of logs)
  - Not a long term solution overall, native IPv6 support is readily available in related applications and should be preferred whenever possible

DHCP (1)

- IPv6 has stateless address autoconfiguration but DHCPv6 (RFC 3315) is available too
- DHCPv6 can be used both for assigning addresses and providing other information like nameserver, ntpserver etc
- If not using DHCPv6 for addresses, no state is required on server side and only part of the protocol is needed. This is called Stateless DHCPv6 (RFC 3736)
- Some server and client implementations only do Stateless DHCPv6 while others do the full DHCP protocol
- The two main approaches are
  - Stateless address autoconfiguration with stateless DHCPv6 for other information
  - Using DHCPv6 for both addresses and other information to obtain better control of address assignment

DHCP (2)

- One possible problem for DHCP is that DHCPv4 only provides IPv4 information (addresses for servers etc) while DHCPv6 only provides IPv6 information. Should a dual-stack host run both or only one (which one)?
- Several vendors working on DHCP but only a few implementations available at the moment
  - DHCPv6 http://dhcpv6.sourceforge.net/
  - dibbler http://klub.com.pl/dhcpv6/
  - NEC, Lucent etc. are working on their own implementations
  - KAME – only stateless
- Cisco routers have a built-in stateless server that provides basic things like nameserver and domain name (also SIP server options in image I checked).
- DHCP can also be used between routers for prefix delegation (RFC 3633). There are several implementations. E.g. Cisco routers can act as both client and server

Remote access via IPv6

- Use native connectivity –
  - Rather easy if you are operating dial-in pool or you are an ADSL service provider
- Use 6to4 if you have global IPv4 address
  - Good 6to4 relay connectivity is a must
- Use tunnelbroker service – rather suboptimal
- Use OpenVPN