Campus Environment

The Campus network is divided into 6 elements that are maintained by IST. These elements are the External, Core, Wireless Core, Data Centre, Distribution, and Access layer (which includes wired and wireless access).

The External, Core, Wireless Core, Data Centre, and Distribution layers are configured and designed with High Availability utilizing redundant hardware, redundant paths and fibre diversity.

Historically, configuration and maintenance of the campus network access layer was distributed amongst the faculties or groups. As a result, the 'standard design' was for one router within each faculty to service all buildings under their responsibility; in limited areas two routers running virtual router redundancy protocol (VRRP) were deployed. The standard single router deployment, for example, would have the router "eng-rt-e2" physically located in the Engineering 2 (E2) building act as the single gateway and route point for all users in most Engineering buildings. In other words, all network access (both wired and wireless) in buildings such as Carl A. Pollock Hall (CPH), Engineering II (E2), Engineering III (E3), and Douglas Wright Engineering (DWE), to name a few, are dependent on their single uplinks to this router and rely on the routers availability for any connectivity to network resources. This environment is not unique to Engineering and exists for all constituencies and many buildings on campus.

Furthermore, although these 'constituency routers' are dually connected to the distribution layer the fibre paths are not diverse and are often connected on adjacent pairs of fibre within the same bundles.

Risks

A failure at the access layer may cause a prolonged loss of Wired and Wireless network connectivity for all buildings and users directly or indirectly connected to the affected device. Within the context of the Information Technology Disaster Recovery Planning (IT DRP), only major events that destroy facilities, destroy equipment, or make a significant amount of IT infrastructure unusable for a prolonged period, are considered. Minor events, such as the failure of an individual power supply or server, are handled as part of routine IT operations, and are not considered part of IT DRP.

Three risks have been identified that would be considered a major event resulting in a prolonged loss of network connectivity at the access layer.

These risks and their likelihood (from DRP definitions) are:

Risk	Likelihood
Fire	Rare (will only occur in exceptional circumstances)
Construction Accident/Fibre Cut	Unlikely (not likely to occur within 3 years)

Human Error/Accidental Fibre Damage [ie unrelated work in service tunnels	Unlikely (not likely to occur within 3 years)

Fibre uplinks are most susceptible to physical damage and would cause a prolonged loss of Wired and Wireless network connectivity based on the risks outlined above. Based on the historical design of the campus building connections, this type of major event could impact one or more constituencies across many or all buildings.

Strategy

IST's strategy is to reduce the risk that will result in a prolonged loss of Wired and Wireless network connectivity while simultaneously reducing the breadth of impact of both major and minor events.

Risk reduction will be accomplished by installing fibre utilizing diverse paths (to the extent possible) directly from the distribution routers located in Physics (PHY) and Math and Computers (MC) to the location of the currently existing routers.

The impact and scope of a major event (and minor events) will be reduced with the installation of building specific routers, dually connected with their own independent and diverse fibre paths to the distribution layer. With the installation of building specific routers, the loss of Wired and Wireless connectivity associated with a major event at the building router layer is limited to the specific building experiencing the event and requires two independent events to occur for a complete loss of connectivity for both paths.

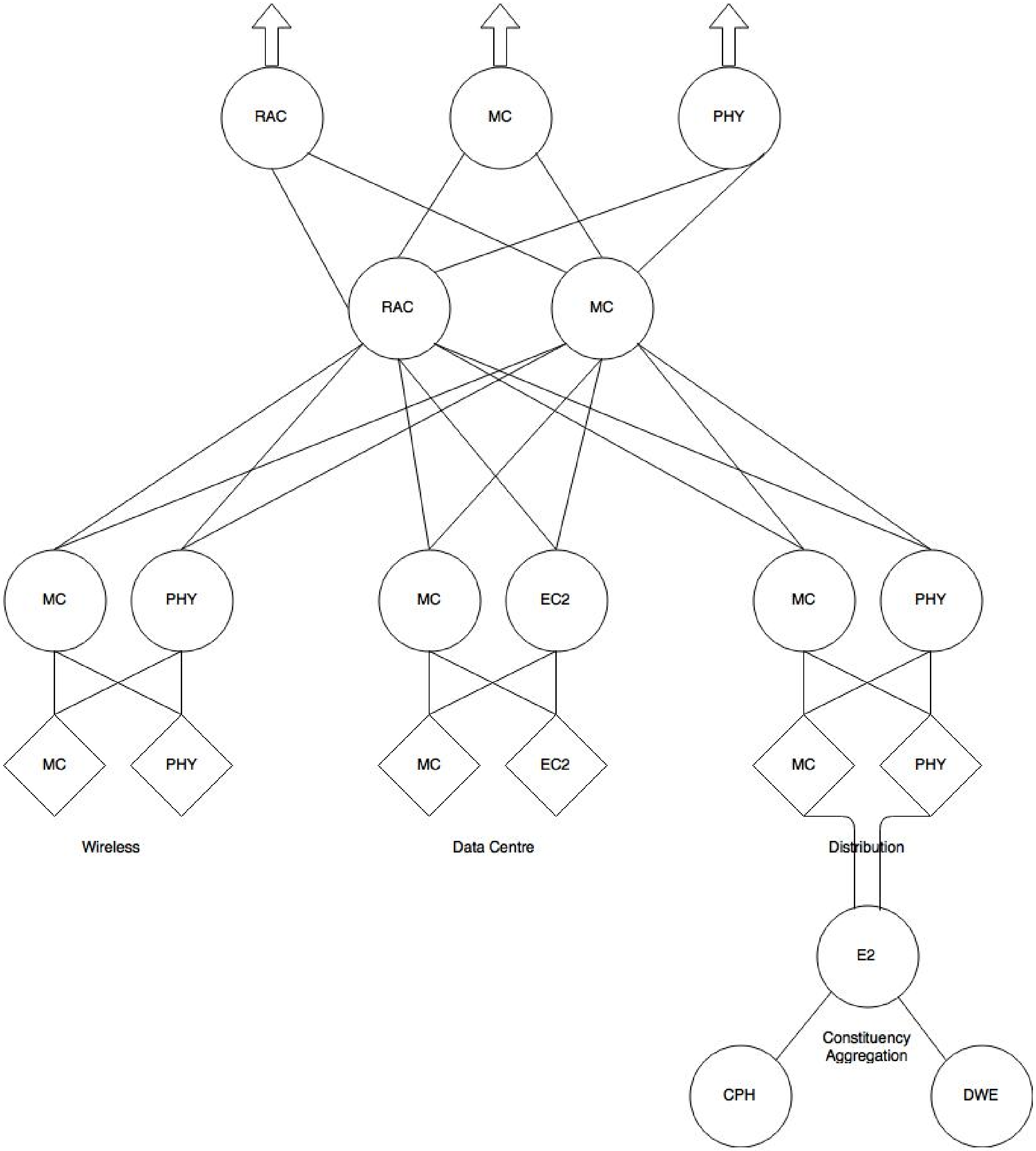
To support independent building routers, Layer3 networks (IP subnets) must be contained and isolated within a building. This will require coordination, support and resources from the faculties to renumber existing hosts. To minimize future efforts and duplication of work any new assignments and subnet planning should be designed as though these routers exist and are in service. IST has been attempting to perform this practise for many years and this separation already exists for many buildings on campus.

This strategy excludes 'Data Centres/Server rooms" but it is recommended that each design be reviewed independently against their own unique requirements.

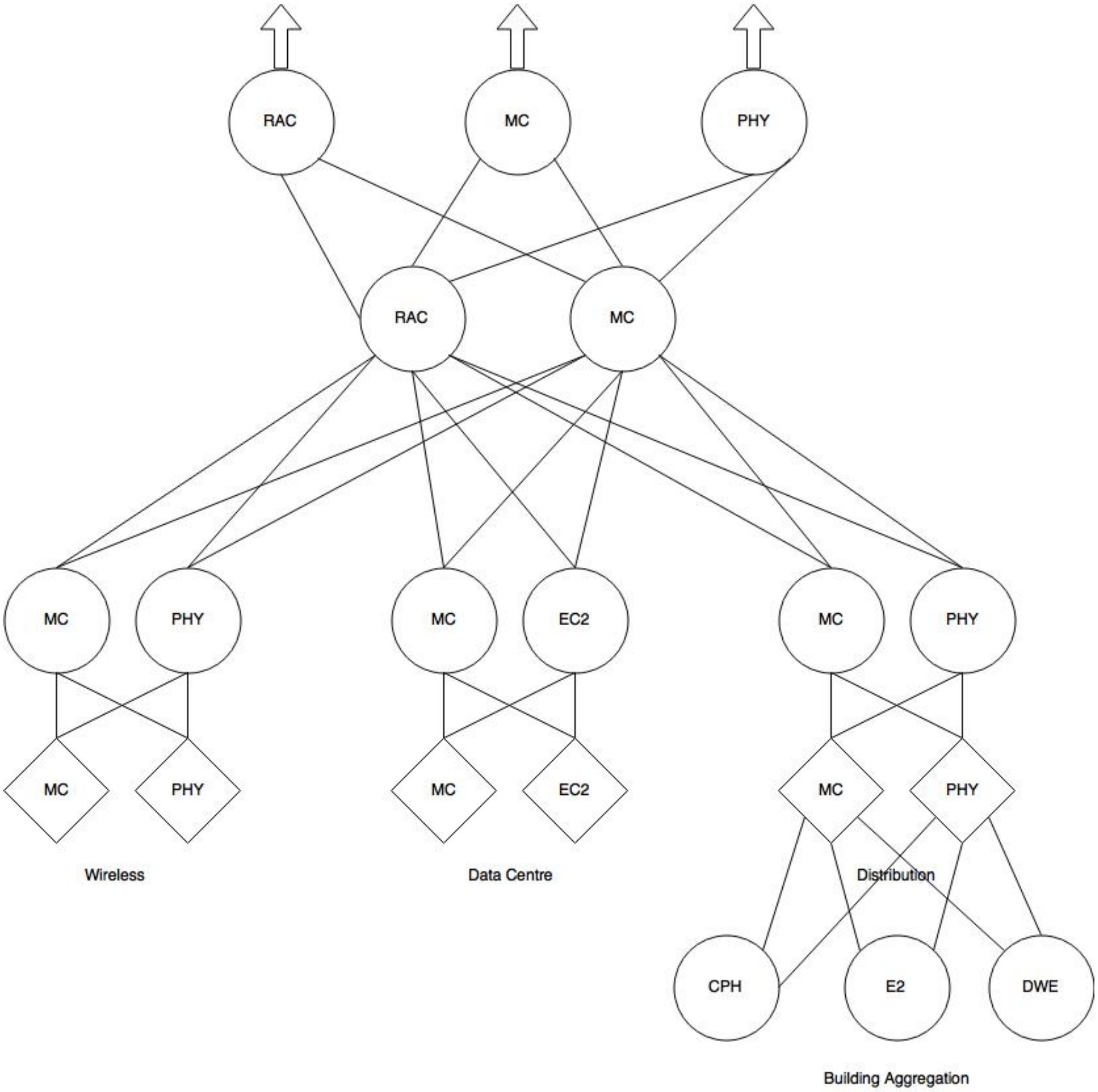
Results

Due to the rare and unlikely chance of the identified risks and the effort required to renumber some remaining areas and resources required to install the redundant fibre paths, IST is proposing that the identified risks are acceptable until the campus wide building routers are implemented, the diverse fibre paths are installed and the remaining networks and buildings are logically separated.

Without Fibre Diversity or Building Routers:



With Fibre Diversity and Building Routers:


RAC
MC
PHY
RAC
MC
MC
PHY
MC
EC2
MC
PHY
MC
PHY
MC
EC2
MC
PHY
Wireless
Data Centre
Distribution
CPH
E2
DWE
Building Aggregation