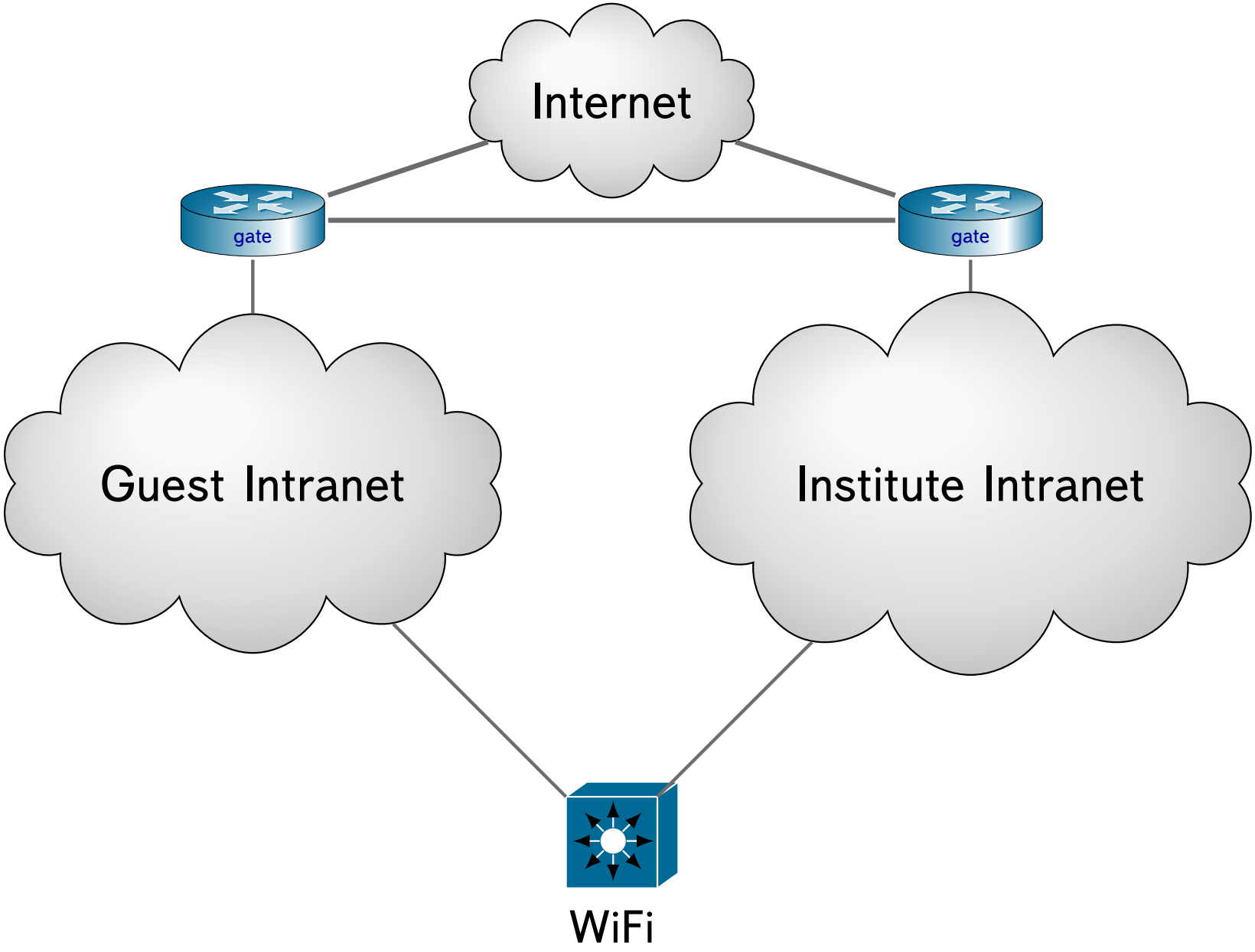
Концепция построения общеинститутской WiFi сети ПИЯФ

Цели

- Создание двух изолированных WiFi сетей:
  - Сети пользователей института интегрированной с локальными сетями отделений
  - Гостевой сети полностью изолированной от сетей внутри института
- Построение сети WiFi-точек доступа с возможностью передвижения между корпусами, с сохранением своего ip адреса и привилегий доступа


Internet
gate
gate
Guest Intranet
Institute Intranet
WiFi

VLAN

– логическая («виртуальная») локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети.

Текущее состояние WiFi сетей института

- Отсутствие какой бы то ни было единой сети
- Каждая точка доступа имеет свои настройки и свой тип авторизации или отсутствие онного (есть открытые точки)
- Большинство точек имеют свои серые сети с NAT – нельзя понять кто есть кто в сети
- Нет разделения на гостевую и не гостевую WiFi сети

Концепция развития WiFi сети института

- Единая авторизация пользователей сети WiFi
- Доступ сотрудников подключённых к сети WiFi ко всем внутренним сервисам отделений и общеинститутским сервисам
- Отдельная гостевая сеть с прямым доступом в интернет изолированная от общеинститутских сетей

Концепция изолированной гостевой сети

- Гостевая сеть находится в отдельном VLAN без доступа к внутренней сети института
- Гостевая сеть обеспечивает только базовый доступ в интернет ??? (HTTP/HTTPS/SSH/IMAP/POP3/SMTP?)
- Гостевая сеть не требует какую либо особую авторизацию????

Концепция WiFi сети института

- Базовая WiFi сеть института, обеспечивает доступ к внутренним сервисам отделений и общеинститутским сервисам, в соответствии с внутренней политикой института и отделений
- Для доступа к сети требуется централизованная авторизация пользователей
- Обеспечивает доступ к Интернет и другим сервисам в соответствии с внутренней политикой института
- Сети отделений находятся в отдельных маршрутизированных VLAN

Какие требуются компоненты для общей WiFi сети

- Сервис авторизации гостей и пользователей
- Сеть точек доступа WiFi с роумингом и едиными параметрами доступа
- Средства обеспечения подключения точек доступа WiFi к сети института и гостевой сети
  - Кабельная сеть института
  - Средства маршрутизации точек и подключённых к ним пользователей по VLAN в зависимости от параметров авторизации

Сервис авторизации

- Мастер сервер хранящий базу пользователей, устройств и параметров их доступа
- Сервисная сеть для точек доступа WiFi
- Администрирование сервиса авторизации
- Минимальный HelpDesk

Авторизация пользователей и гостей

- Для сотрудников
  - Устройство должно быть известно (MAC адрес есть в база института)
  - (Опционально?) у пользователя есть пара логин/пароль и/или сертификат
  - Устройство получает настройки в соответствии с персональными параметрами пользователя и попадает в соответствующий VLAN (например VLAN отделения)
- Для гостей
  - Если устройство не известно то пользователь попадает в гостевую сеть (MAC адрес устройства не числится в базе института)
  - В гостевой сети ему присваиваются временный IP

Сеть точек доступа WiFi

- Точки работают в режиме моста
- Точки имеют единые параметры авторизации
- Точки должны иметь поддержку VLAN
- Должен быть обеспечен роуминг между точками доступа
- Точки доступа должны быть подключены к управляемым коммутаторам с поддержкой VLAN
- Требуется обеспечить маршрутизацию VLAN между корпусами

Администрирование пользователей и оборудования

- Новый пользователь
  - Подаёт заявку ответственному за регистрацию пользователей
  - Только одна подпись или Электронная форма
  - В заявке указывается E-mail
  - Возможно указание нескольких MAC-адресов устройств при начальной регистрации
  - Пользователю на почту приходит подтверждение
- Старый пользователь
  - Может добавлять/удалять свои устройства через портал
  - Ограничение на 5-10 одновременно зарегистрированных устройств
- Администрирование
  - Администраторы отделов могут добавлять/удалять пользователей и их устройства для своего отделения
  - Администраторы системы могут добавлять/удалять любых пользователей в том числе администраторов отделов

Создание тестовой сети WiFi

Предлагается создать тестовую сеть WiFi на базе отделений ОМРБ и ОИТА на которой протестировать подход и развёртывание общеинститутской сети WiFi