
OTUS
ОНЛАЙН-ОБРАЗОВАНИЕ
Онлайн-образование

Не забыть включить запись!

Меня хорошо видно && слышно?

Ставьте + , если все хорошо
Напишите в чат, если есть проблемы

Проектирование и управление сетью

Правила вебинара

Активно участвуем

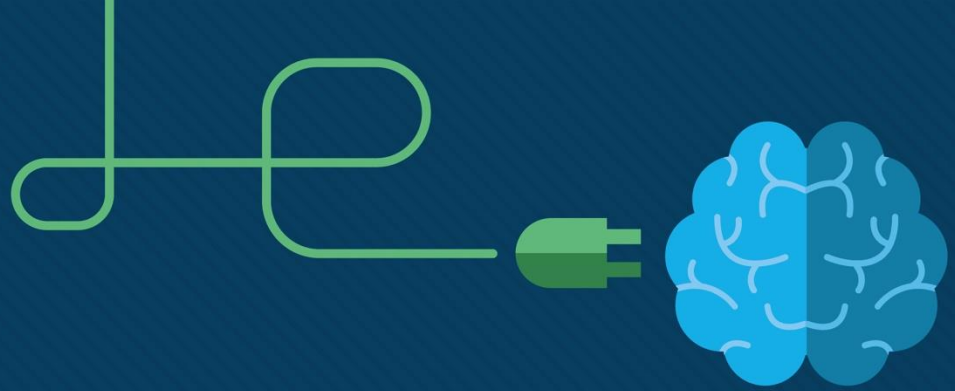
Задаем вопрос в чат или голосом

Off-topic обсуждаем в Slack #канал группы или #general

Вопросы вижу в чате, могу ответить не сразу

Карта курса

WWW.OTUS.RU



Модуль 10: Управление сетью

Корпоративные сети, безопасность и автоматизация v7.0 (ENSA)

10.1. Обнаружение устройств с помощью протокола CDP

Общие сведения о протоколе CDP

Протокол Cisco Discovery Protocol (CDP) — это проприетарный протокол компании Cisco уровня 2, который служит для сбора информации об устройствах Cisco, использующих один и тот же канал передачи данных. CDP не зависит от среды передачи данных и других протоколов; он включен на всех устройствах Cisco, таких как маршрутизаторы, коммутаторы и серверы доступа.

Устройство периодически отправляет объявления CDP на подключенные устройства. Посредством объявлений осуществляется обмен информацией о типах обнаруженных устройств, их именах, количестве и типах интерфейсов.

Настройка и проверка протокола CDP

- На устройствах Cisco протокол CDP включен по умолчанию. Чтобы проверить состояние CDP и отобразить сведения о нем, введите команду **show cdp**.
- Чтобы отключить CDP для определенного интерфейса, например используемого для подключения к интернет-провайдеру, введите **no cdp enable** в режиме настройки интерфейса. Протокол CDP по-прежнему включен на устройстве, однако объявления CDP больше не передаются через этот интерфейс. Чтобы снова включить CDP для определенного интерфейса, введите **cdp enable**
- Чтобы включить CDP сразу для всех поддерживаемых интерфейсов устройства, введите команду **cdp run** в режиме глобальной конфигурации. Чтобы отключить CDP сразу для всех интерфейсов устройства, введите команду **no cdp run** в режиме глобальной конфигурации.
- Команда **show cdp interface** отображает интерфейсы устройства, на которых включен протокол CDP. Кроме того, выводится состояние каждого интерфейса.

Поиск устройств с помощью протокола CDP

- Если в сети включен протокол CDP, структуру сети можно определить с помощью команды **show cdp neighbors**.
- Выходные данные показывают, что к интерфейсу G0/0/1 на R1 подключено другое устройство Cisco S1. Кроме того, S1 подключается через F0/5

```
R1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID Local Intrfce Holdtme Capability Platform Port ID
S1 Gig 0/0/1 179 S I WS-C3560- Fas 0/5
```

Поиск устройств с помощью протокола CDP (продолжение)

Администратор сети использует **сведения show cdp neighbors** для обнаружения IP-адреса S1. Как показано в выходных данных, адрес S1 — 192.168.1.2.

```
R1# show cdp neighbors detail
-------------------------
Device ID: S1
Entry address(es):
  IP address: 192.168.1.2
Platform: cisco WS-C3560-24TS, Capabilities: Switch IGMP
Interface: GigabitEthernet0/0/1, Port ID (outgoing port): FastEthernet0/5
Holdtime : 136 sec

(дальше выходные данные опущены)
```

10.2. Обнаружение устройств с помощью протокола LLDP

Общие сведения о протоколе LLDP

Протокол LLDP — это не зависящий от производителя протокол для обнаружения соседей, подобный CDP. LLDP работает с сетевыми устройствами, такими как маршрутизаторы, коммутаторы и точки доступа к беспроводной сети LAN. Этот протокол объявляет себя и свои возможности другим устройствам и получает данные от физически подключенных устройств уровня 2.

Настройка и проверка протокола LLDP

- На устройствах Cisco протокол LLDP может быть включен по умолчанию. Чтобы включить LLDP для всех интерфейсов сетевого устройства Cisco, введите команду **lldp run** в режиме глобальной конфигурации. Чтобы отключить протокол LLDP, введите команду **no lldp run** в режиме глобальной конфигурации.
- Как и протокол CDP, протокол LLDP можно включить и отключить на конкретных интерфейсах. Однако передачу и прием пакетов LLDP необходимо настраивать отдельно.
- Чтобы убедиться в том, что протокол LLDP был включен на устройстве, введите команду **show lldp** в привилегированном режиме EXEC.

```
Switch# conf t
Введите построчно команды настройки. В конце нажмите CNTL/Z.
Switch(config)# lldp run
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch(config-if)# end
Switch# show lldp
Global LLDP Information:
   Status: ACTIVE
   LLDP advertisements are sent every 30 seconds
   LLDP hold time advertised is 120 seconds
   LLDP interface reinitialisation delay is 2 seconds
```

Поиск устройств с помощью протокола LLDP

Если включен протокол LLDP, можно найти соседей определенного устройства с помощью команды **show lldp neighbors**.

```
S1# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID Local Intf Hold-time Capability Port ID
R1 Fa0/5 117 R Gi0/0/1
S2 Fa0/1 112 B Fa0/1
Total entries displayed: 2
```

Поиск устройств с помощью протокола LLDP

Если нужна более подробная информация о соседних устройствах, можно воспользоваться командой **show lldp neighbors detail**, которая предоставляет такие сведения, как версии IOS, IP-адреса и функции соседних устройств.

```
S1# show lldp neighbors detail
------------------------------------------------
Chassis id: 848a.8d44.49b0
Port id: Gi0/0/1
Port Description: GigabitEthernet0/0/1
System Name: R1
System Description: Cisco IOS Software [Fuji], ISR Software (X86_64_LINUX_.....,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 22-Aug-19 18:09 by mcpre

Time remaining: 111 seconds
System Capabilities: B,R
Enabled Capabilities: R
Management Addresses - not advertised
(дальше выходные данные опущены)
```

10.3 NTP

Службы времени и календаря

- Основным источником информации о времени в системе являются программные часы маршрутизатора или коммутатора, Это основной источник времени для системы. Синхронизирует время на всех устройствах в сети. Если время на устройствах не синхронизировано, определить порядок событий и их причину невозможно.
- Как правило, параметры даты и времени на маршрутизаторе или коммутаторе можно задать одним из двух способов. Можно вручную настроить дату и время, как показано в примере, или настроить протокол сетевого времени (NTP).

```
R1# clock set 20:36:00 nov 15 2019
R1#
*Nov 15 20:36:00.000: %SYS-6-CLOCKUPDATE: System clock has been
updated from 21:32:31 UTC Fri Nov 15 2019 to 20:36:00 UTC Fri Nov 15
2019, configured from console by console.
```

Службы времени и календаря (продолжение)

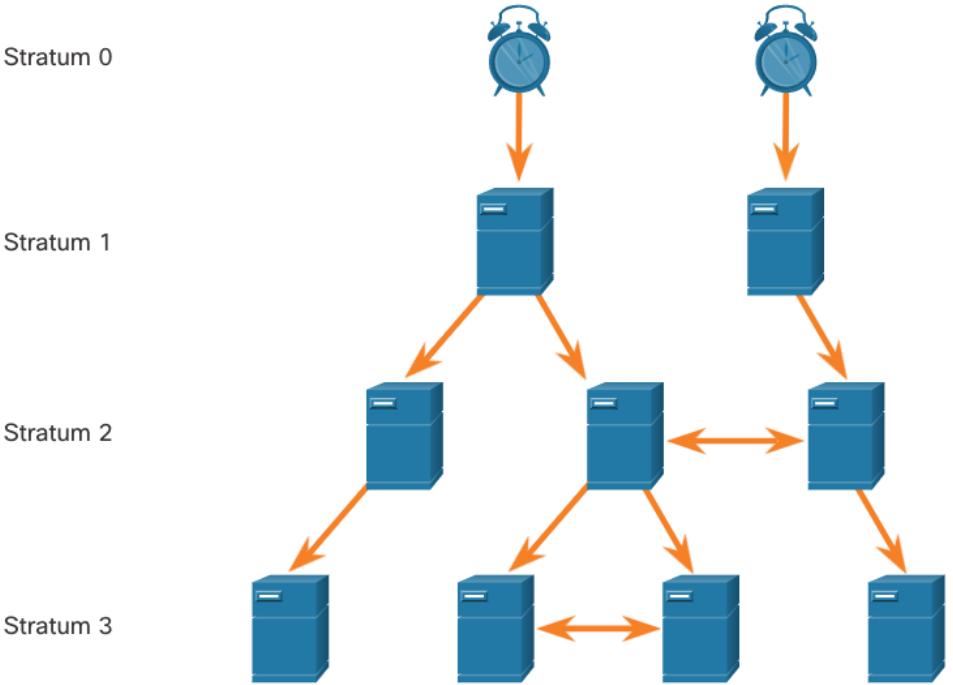
По мере роста сети становится все труднее обеспечивать синхронизацию времени на всех устройствах инфраструктуры.

Более эффективным решением является настройка в сети протокола NTP. Этот протокол позволяет маршрутизаторам в сети синхронизировать свои настройки времени с NTP-сервером, что обеспечивает более согласованные настройки времени. NTP можно настроить для синхронизации с частным генератором тактовых импульсов или общедоступным сервером NTP в Интернете. Протокол NTP использует порт UDP 123 и задокументирован в RFC 1305.

Принципы работы протокола NTP

В сетях NTP используется иерархическая система источников времени. Каждый уровень этой иерархической системы называется часовым слоем (stratum). Уровень часового слоя определяется как количество переходов от доверенного источника. Для распределения синхронизированной информации о времени по сети используется протокол NTP.

Максимальное количество переходов равно 15. Часовой слой 16 имеет самый низкий уровень и указывает на то, что устройство не синхронизировано.



Принципы работы протокола NTP

- **Устройства слоя 0:** Эти доверенные источники времени, также называемые устройствами часового слоя 0, являются высокоточными устройствами хранения времени, которые считаются точными и работают практически без задержек.
- **Устройства слоя 1** подключены напрямую к доверенным источникам времени. Они выступают в роли основного стандарта сетевого времени.
- **Слой 2 и ниже.** Серверы слоя 2 подключены к устройствам слоя 1 через сеть. Устройства часового слоя 2, например клиенты NTP, синхронизируют свое время с помощью пакетов NTP, которые они получают от серверов часового слоя 1. Эти устройства могут также выступать в роли серверов для устройств часового слоя 3.

Серверы времени, находящиеся в одном часовом слое, могут работать как равноправные серверы времени на одном уровне часового слоя для обеспечения резервирования или проверки правильности времени.

Настройка и проверка протокола NTP

- Перед настройкой протокола NTP в сети введите команду **show clock**, которая отображает текущее время программных часов. При выборе параметра « **detail** » обратите внимание, что источником времени является пользовательская конфигурация. Это означает, что время было настроено вручную с помощью команды **clock** .
- Используйте команду **ntp server** *ip-адрес* в режиме глобальной конфигурации, чтобы указать адрес 209.165.200.225 в качестве сервера NTP для маршрутизатора R1. Чтобы убедиться, что в качестве источника времени выбран NTP, выполните команду **show clock detail**. Обратите внимание, что теперь источником времени является NTP.

```
R1# show clock detail
20:55:10.207 UTC Fri Nov 15 2019
Time source is user configuration
R1# config t
R1(config)# ntp server 209.165.200.225
R1(config)# end
R1# show clock detail
21:01:34.563 UTC Fri Nov 15 2019
Time source is NTP
```

Настройка и проверка протокола NTP

Команды **show ntp associations** и **show ntp status**, которые позволяют проверить, что маршрутизатор R1 синхронизирован с сервером NTP по адресу 209.165.200.225. Обратите внимание: маршрутизатор R1 синхронизирован с сервером NTP часового слоя 1 по адресу 209.165.200.225, который синхронизирован с часами GPS. Команда **show ntp status** показывает, что теперь маршрутизатор R1 является устройством часового слоя 2, которое синхронизировано с сервером NTP по адресу 209.165.220.225.

```
R1# show ntp associations

address ref clock st when poll each delay offset disp
*~209.165.200.225 .GPS.        1 61 64 377 0.481 7.480 4.261
• sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

R1# show ntp status
Clock is synchronized, stratum 2, reference is 209.165.200.225
nominal freq is 250.0000 Hz, actual freq is 249.9995 Hz, precision is 2**19
(дальше выходные данные опущены)
```

Настройка и проверка протокола NTP

- Часы S1 настроены на синхронизацию с R1 с помощью команды **ntp server**, а конфигурация проверяется с помощью команды **show ntp ассоциаций**
- Команда **show ntp associations** позволяет убедиться, что часы на S1 теперь синхронизированы с R1 с адресом 192.168.1.1 по протоколу NTP. Коммутатор S1 теперь является устройством часового слоя 3, которое может предоставлять службу NTP для остальных устройств в сети, например оконечных устройств.

```
S1(config)# ntp server 192.168.1.1
S1(config)# end
S1# show ntp associations
address ref clock st when poll reach delay offset disp
*~192.168.1.1 209.165.200.225 2 12 64 377 1.066 13.616 3.840
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
(дальше выходные данные опущены)

S1# show ntp status
Clock is synchronized, stratum 3, reference is 192.168.1.1
nominal freq is 119.2092 Hz, actual freq is 119.2088 Hz, precision is 2**17
(output omitted
```

10.4 Проткол SNMP

Знакомство с SNMP

Протокол SNMP позволяет осуществлять управление и мониторинг устройств в сети IP. С его помощью сетевые администраторы могут осуществлять мониторинг производительности сети, находить и устранять проблемы, планировать рост сети.

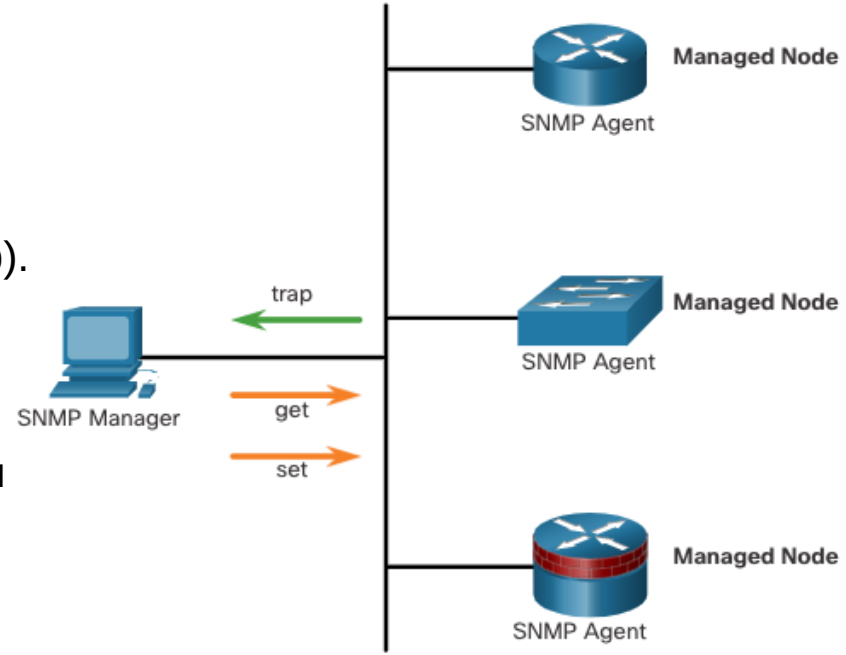
SNMP — это протокол уровня приложений, предоставляющий формат сообщения для обмена данными между диспетчерами и агентами. Система SNMP состоит из следующих трех элементов.

- диспетчер SNMP;
- агенты SNMP (управляемый узел);
- информационная база управления (MIB)

SNMP определяет способ обмена информацией об управлении между приложениями управления сетями и агентами управления. Диспетчер SNMP опрашивает агенты и запрашивает в MIB информацию об агентах SNMP через порт UDP 161. Агенты SNMP отправляют все ловушки SNMP в диспетчер SNMP на порт UDP 162.

Введение в SNMP (продолжение)

- Диспетчер SNMP является частью системы управления сетями (network management system — NMS). Диспетчер SNMP может собирать данные от агента SNMP с помощью запроса get и изменять настройки на агенте с помощью запроса set. Агенты SNMP могут пересылать информацию непосредственно в диспетчер сети, используя ловушки (пакеты trap).
- Агент SNMP и база данных MIB размещены на клиентских устройствах SNMP. В базах данных MIB хранятся данные об устройствах и их функционировании. Они должны быть доступны для прошедших аутентификацию удаленных пользователей. Агент SNMP отвечает за предоставление доступа к локальной базе данных MIB.



Функционирование протокола SNMP

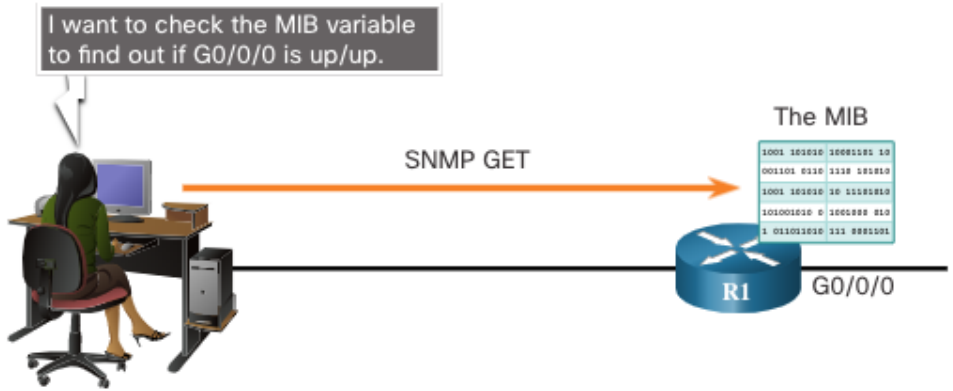
- Агенты SNMP, размещенные на управляемых устройствах, собирают и сохраняют информацию об устройстве и его работе. Затем диспетчер SNMP использует агент SNMP для доступа к сведениям, хранящимся в базе MIB.
- Существует два основных запроса диспетчера SNMP — get и set. В дополнение к конфигурации набор может вызвать действие, например перезапуск маршрутизатора.

Операция	Описание
get-request	Получает значение из определенной переменной.
get-next-request	Получает значение из переменной в таблице; диспетчер SNMP не обязательно должен знать точное имя переменной. Чтобы найти необходимую переменную в таблице, выполняется последовательный поиск.
get-bulk-request	Получает большие блоки данных, например несколько строк в таблице, что обычно требует передачи многочисленных небольших блоков данных. (Работает только с SNMPv2 или более поздней версии.)
get-response	Отвечает на запросы **get-request, get-next-request** и **set-request**, отправляемые системой NMS.
set-request	Сохраняет значение в определенной переменной.

Функционирование протокола SNMP

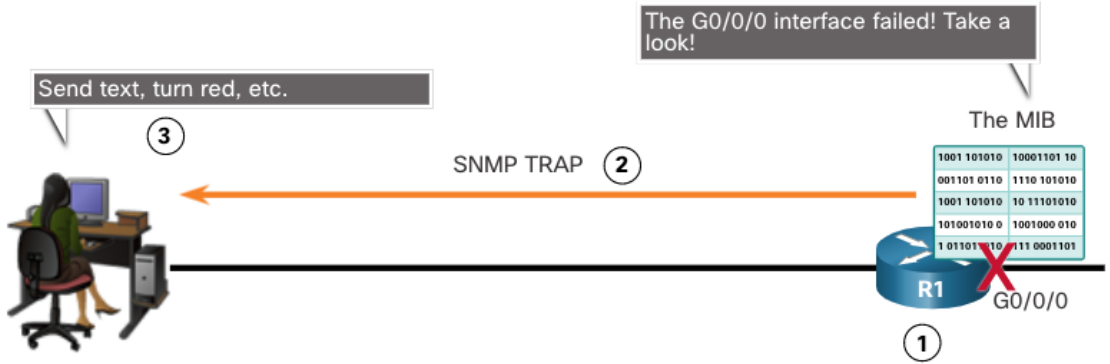
Агент SNMP отвечает на запросы диспетчера SNMP следующим образом.

- **Получение переменной MIB.** Агент SNMP выполняет эту функцию в ответ на запрос GetRequest-PDU от диспетчера сети. Агент получает значение запрошенной переменной MIB и передает это значение в диспетчер сети.
- **Изменение переменной MIB.** Агент SNMP выполняет эту функцию в ответ на запрос SetRequest-PDU от диспетчера сети. Агент SNMP изменяет значение переменной MIB на значение, указанное диспетчером сети. Ответ агента SNMP на запрос set включает новые параметры в устройстве.



Ловушки агента SNMP

- Ловушки — это незапрашиваемые сообщения, предупреждающие диспетчера SNMP о каком-либо условии или событии в сети. Уведомления, направленные на ловушки, помогают сократить использование ресурсов сети и агентов, устраняя необходимость в некоторых запросах на опрос SNMP.
- На рисунке показано использование ловушки SNMP для уведомления сетевого администратора о сбое интерфейса G0/0. Программное обеспечение NMS может отправлять сетевым администраторам текстовые сообщения, отображать всплывающие окно поверх ПО NMS или включать красный значок маршрутизатора в графическом интерфейсе пользователя NMS.



Версии SNMP

- SNMPv1 - устаревший стандарт, определенный в RFC 1157. Использует простой метод проверки подлинности на основе строки сообщества. Не следует использовать из-за рисков безопасности.
- SNMPv2c - определяется в RFCs 1901-1908. Использует простой метод проверки подлинности на основе строки сообщества. Содержит опции массового извлечения, а также более подробные сообщения об ошибках.
- SNMPv3 - определяется в RFCs 3410-3415. Использует аутентификацию пользователя, обеспечивает защиту данных с помощью HMAC-MD5 или HMAC-SHA и шифрование с использованием DES, 3DES или AES шифрования.

Строки сообщества

В версиях SNMPv1 и SNMPv2c для контроля доступа к MIB используется модель строки сообщества (community string). Строки сообщества представляют собой незашифрованный пароль. Строки сообщества SNMP производят аутентификацию доступа к объектам MIB.

Существует два типа строк сообщества:

- **Только чтение (Read-only — ro)** — предоставляет доступ к переменным MIB, но не позволяет менять эти переменные. Поскольку версия 2c предоставляет минимальную безопасность, многие организации используют SNMPv2c в режиме только для чтения.
- **Чтение и запись (Read-write — rw)**. Предоставляет доступ для чтения и записи ко всем объектам в MIB.

Чтобы просмотреть или настроить переменные MIB, пользователь должен указать тип соответствующей строки сообщества — для чтения или для записи.

Идентификатор объекта MIB

Переменные в MIB организованы иерархически. Фактически MIB определяет каждую переменную в качестве идентификатора объекта (OID). Идентификаторы OID уникальным образом определяют управляемые объекты. MIB организует OID на основе стандартов RFC, формируя иерархию OID, которая обычно представляется в виде дерева.

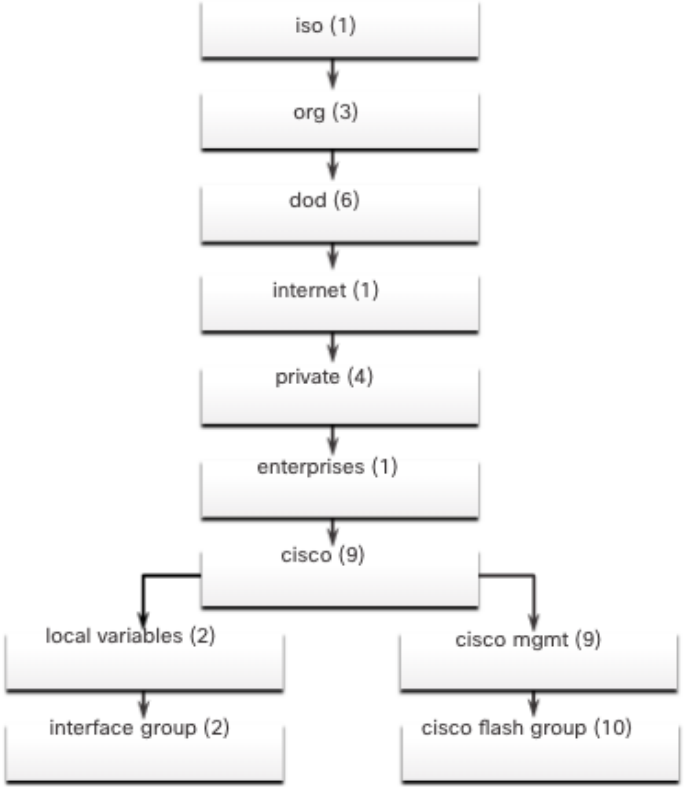
- Дерево базы MIB для любого устройства включает несколько ветвей с переменными, общими для многих сетевых устройств, и несколько ветвей с уникальными переменными конкретного устройства или поставщика.
- Некоторые общедоступные переменные определены в документах RFC. Большинство устройств используют эти переменные MIB. Кроме того, поставщики сетевого оборудования, такие как Cisco, могут определять собственные частные ветви дерева для добавления новых переменных, которые будут использоваться только для их устройств.

Идентификатор объекта MIB

На рисунке показаны части структуры MIB, определенные Cisco. Обратите внимание, что OID может быть определен с помощью слов или чисел, что помогает найти определенную переменную в дереве.

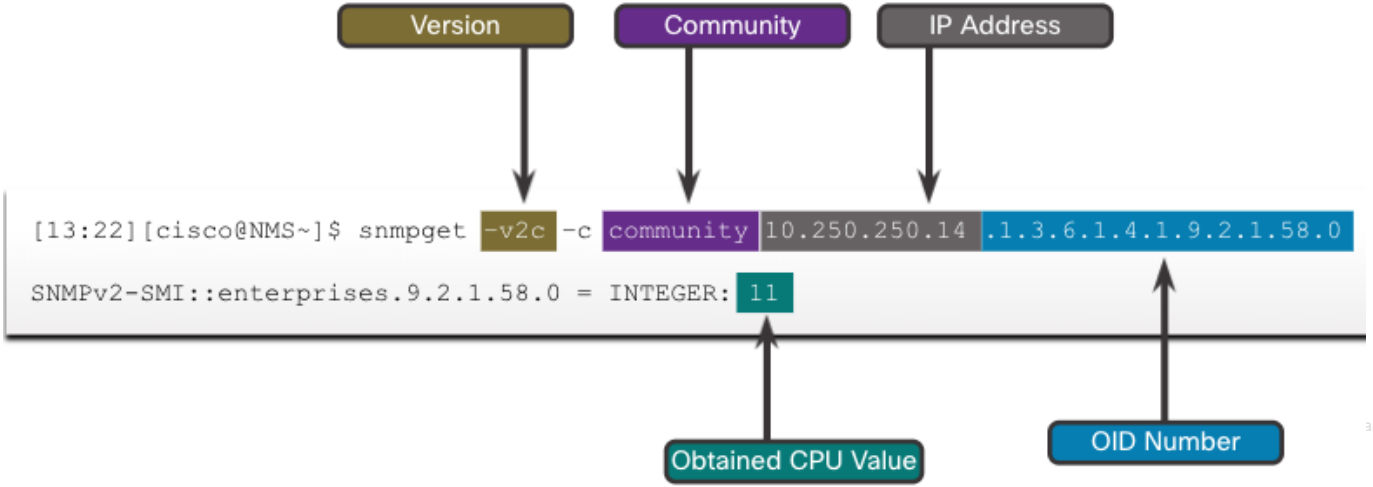
OID, принадлежащие Cisco, пронумерованы следующим образом: .iso (1).org (3).dod (6).internet (1).private (4).enterprises (1).cisco (9).

Таким образом, OID — 1.3.6.1.4.1.9.



Сценарий опроса SNMP

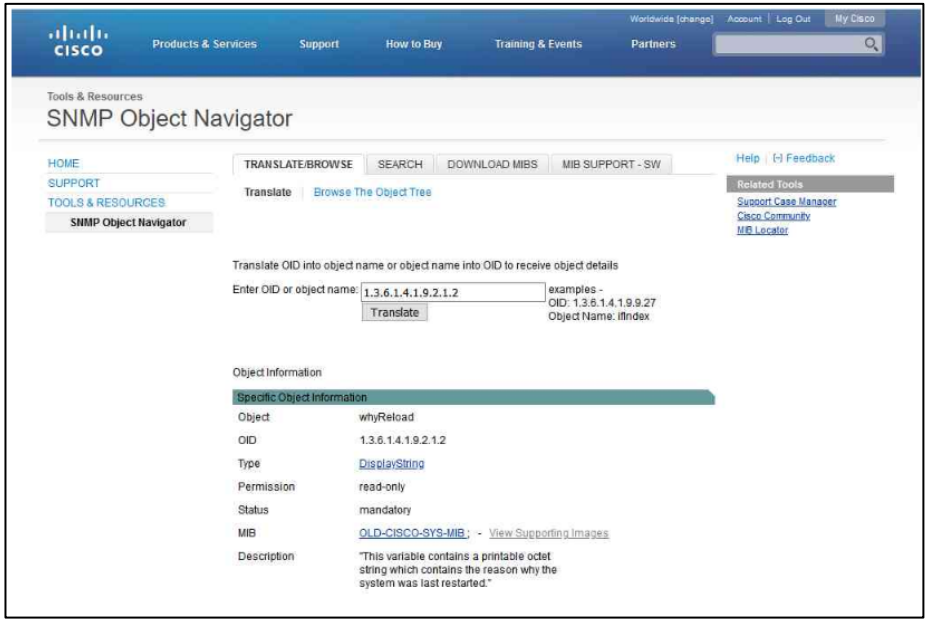
- SNMP может использоваться для наблюдения за ЦП в течение определенного периода времени опрашивающими устройствами. Статистика ЦП собирается в системе NMS и представляется в виде графика.
- Данные извлекаются с помощью служебной программы snmpget и передаются в систему NMS. С помощью утилиты snmpget можно вручную извлекать данные в реальном времени или запустить отчет NMS. Этот отчет даст вам период времени, в течение которого вы можете использовать данные для получения среднего значения.



SNMP Object Navigator

Данная служебная программа дает некоторое представление о базовых механизмах работы SNMP. Однако работа с длинными именами переменных MIB, такими как 1.3.6.1.4.1.9.2.1.58.0, может представлять проблему для обычного пользователя. Чаще всего персонал, обслуживающий сеть, использует решение для управления сетями с простым и удобным графическим интерфейсом пользователя, причем все имена переменных MIB прозрачны для пользователя.

Cisco SNMP Navigator на веб-сайте http://www.cisco.com позволяет исследовать подробности о конкретном OID.



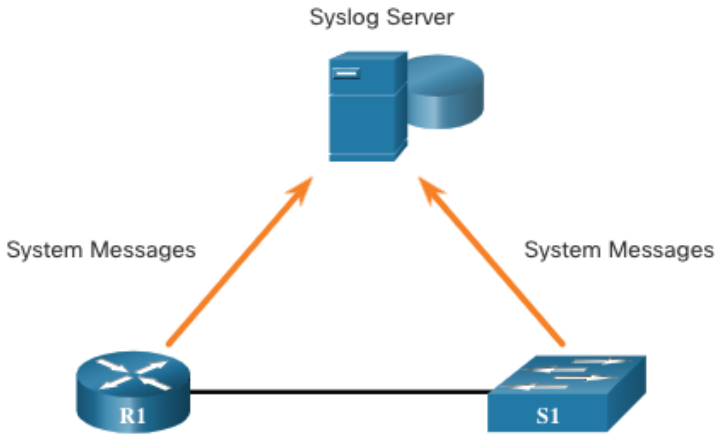
10.5 Системный журнал

Введение в Syslog

Syslog использует порт UDP 514 для отправки сообщений с уведомлением о событиях по сетям IP на средства сбора сообщений о событиях, как показано на рисунке.

Сервис ведения системного журнала выполняет три основные функции:

- сбор информации в журнал для мониторинга и устранения неполадок;
- выбор типа информации, сбор которой будет осуществляться;
- определение получателей собранных сообщений syslog.



Принципы работы с системным журналом

Протокол системного журнала (syslog) начинает с отправки системных сообщений и выходных данных команд **debug** в локальный процесс ведения журналов соответствующего устройства. Конфигурация Syslog может отправлять эти сообщения по сети на внешний сервер syslog, где они могут быть получены без необходимости доступа к фактическому устройству.

Сообщения syslog могут отправляться во внутренний буфер. Их можно просматривать только через интерфейс командной строки устройства.

Наконец, сетевой администратор может указать, какие типы системных сообщений будут отправляться в различные места назначения. В число популярных назначений для сообщений syslog входят следующие:

- буфер ведения журналов (ОЗУ в маршрутизаторе или коммутаторе);
- порт консоли;
- линия терминала;
- сервер Syslog.

Формат сообщений syslog

Устройства Cisco создают сообщения syslog при определенных сетевых событиях. Во всех сообщениях syslog указывается уровень важности (severity level) и объект (facility).
Чем меньше назначаемое число, тем более важным является оповещение syslog. В настройках уровня важности сообщений можно установить, куда отправлять сообщения каждого типа (например на консоль или в другие места назначения).
Полный перечень уровней syslog представлен в таблице.

Название уровня серьезности	Уровень серьезности	Описание
Чрезвычайная ситуация	Уровень 0	Систему нельзя использовать
Предупреждение	Уровень 1	Требуется принять немедленные меры
Критический	Уровень 2	Критическое состояние
Ошибка	Уровень 3	Состояние ошибки
Предупреждение	Уровень 4	Состояние предупреждения
Уведомление	Уровень 5	Нормальное, но требующее внимания состояние
Информационный	Уровень 6	Информационное сообщение
Отладка	Уровень 7	Сообщение отладки

Объекты Syslog

Помимо указания уровня важности в сообщениях syslog также содержатся сведения об объекте. Объекты syslog (syslog facilities) — это идентификаторы сервисов, которые определяют и классифицируют данные о состоянии системы для отчетов об ошибках и событиях. Доступные варианты объектов ведения журнала зависят от конкретного сетевого устройства.

Ниже приведены некоторые из общепринятых объектов сообщений syslog, которые регистрируются на маршрутизаторах Cisco IOS:

- IP
- Протокол OSPF
- Операционная система SYS
- Протокол IPSec
- IP интерфейса (IF)

Объекты Syslog

По умолчанию формат сообщений syslog в ПО Cisco IOS выглядит следующим образом:

%facility-severity-MNEMONIC: description

Пример выходных данных об изменении состояния канала EtherChannel коммутатора Cisco на активное будет выглядеть следующим образом:

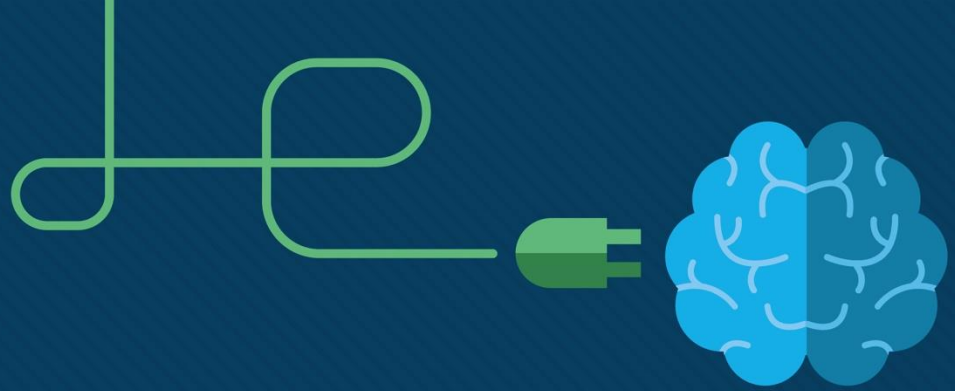
```
%LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

В этом примере объектом является LINK, назначен уровень серьезности 3, в качестве КРАТКОГО КОДА выступает UPDOWN.

Настройка временной метки системного журнала

По умолчанию в сообщениях журнала нет метки времени. Сообщения журнала должны иметь метку времени. Потому что, когда они отправляются следующему адресату, например на сервер системного журнала, появляется запись о создании сообщения. Команда **service timestamps log datetime** позволяет принудительно отображать дату и время для зарегистрированных событий.

```
R1# configure terminal
R1(config)# interface g0/0/0
R1(config-if)# shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to down
R1(config-if)# exit
R1(config)# service timestamps log datetime
R1(config)# interface g0/0/0
R1(config-if)# no shutdown
*Mar 1 11:52:42: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to down
*Mar 1 11:52:45: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up
*Mar 1 11:52:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
changed state to up
R1(config-if)#
```



Модуль 11: Проектирование сети

Корпоративные сети, безопасность и автоматизация
v7.0 (ENSA)

11.1 – Иерархические сети

Необходимость масштабирования сети

Организации все больше полагаются на свои сети, предоставляющие критически важные сервисы.

Развивающиеся организации нуждаются в сетях, которые могут масштабировать и поддерживать:

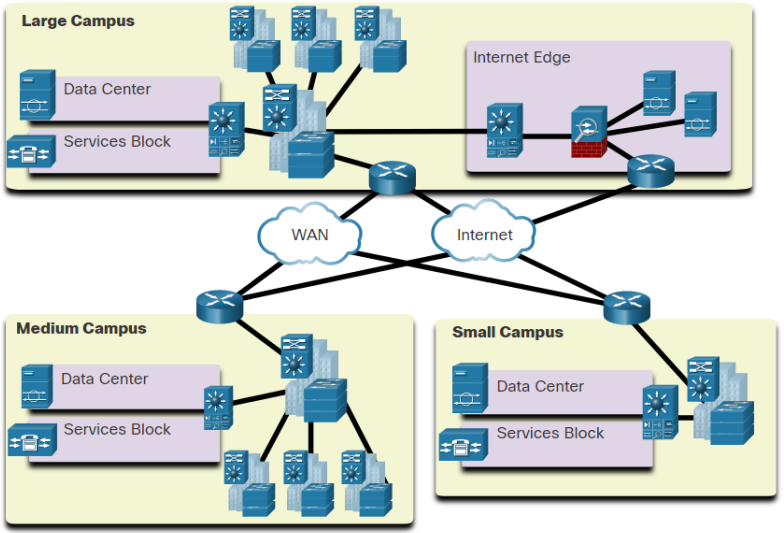
- Конвергентный сетевой трафик
- Критически важные приложения
- Соответствие различным требованиям бизнеса
- Централизованное административное уравление

Архитектуры кампусных сетей могут быть различными: от небольших сетей, состоящих из одного коммутатора локальной сети, до очень больших сетей с тысячами подключений.

Коммутируемые сети без границ

Сети без границ Cisco (Cisco Borderless Network) - это сетевая архитектура, которая может подключать кого угодно, где угодно и когда угодно, на любом устройстве; безопасно, надежно и без проблем.

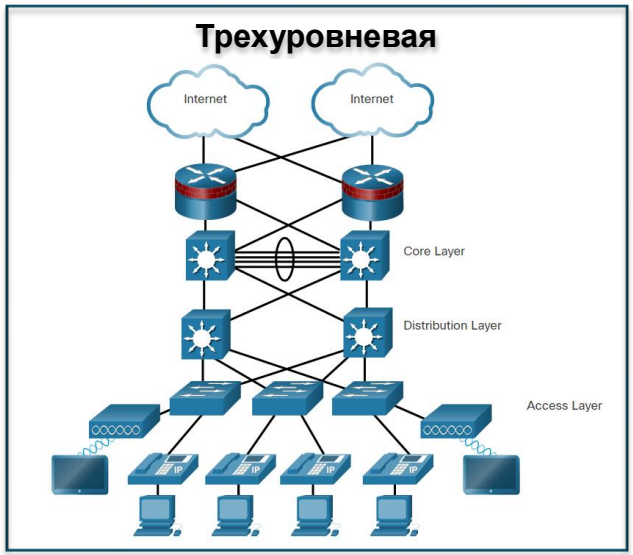
- Она обеспечивает платформу для унификации проводного и беспроводного доступа, построенную на иерархической инфраструктуре оборудования, которая является масштабируемой и отказоустойчивой.
- Коммутируемые сети без границ являются иерархическими, модульными, устойчивыми и гибкими.

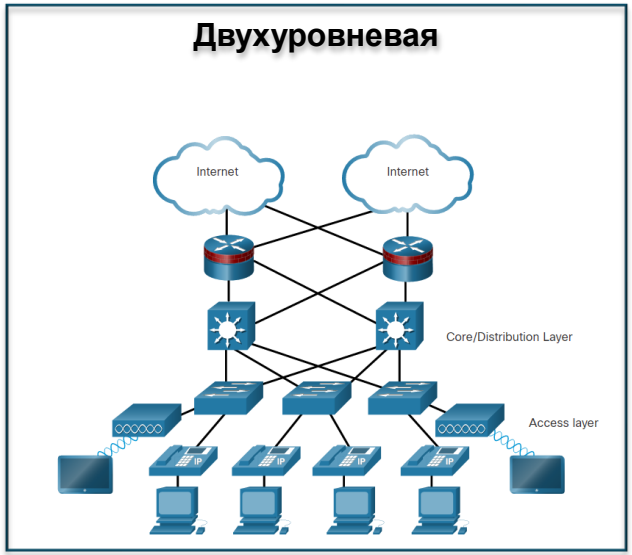


Иерархия в коммутируемой сети без границ

Иерархические сети используют многоуровневый дизайн уровней доступа, распределения и ядра, при этом каждый уровень выполняет четко определенную роль в сети кампуса.

Существуют две проверенные временем иерархические структуры проектирования для кампусных сетей.





Функции уровней доступа, распределения и ядра

Уровень доступа

- Уровень доступа обеспечивает сетевой доступ для пользователей.
- Коммутаторы уровня доступа подключаются к коммутаторам уровня распределения.

Уровень распределения

- Уровень распространения реализует маршрутизацию, качество обслуживания и безопасность.
- Он объединяет крупномасштабные сети проводных шкафов и ограничивает широковещательные домены уровня 2.
- Коммутаторы уровня распределения подключаются к коммутаторам уровня доступа и уровня ядра.

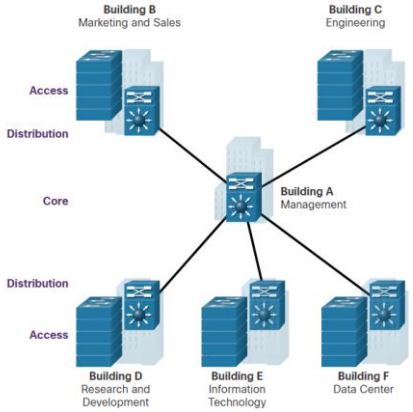
Уровень ядра

- Уровень ядра является магистральной сетью и соединяет несколько уровней сети.
- Уровень ядра обеспечивает изоляцию неисправностей и высокоскоростное магистральное подключение.

Трехуровневые и двухуровневые примеры

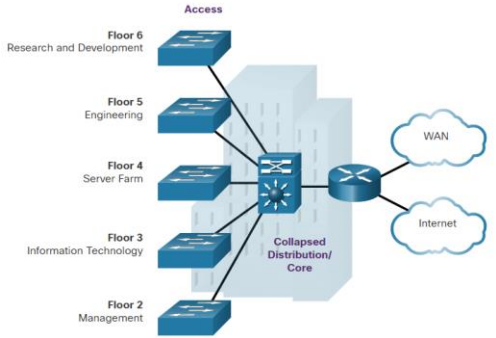
Трехуровневая сеть кампуса

- Используется организациями, требующими уровни доступа, распространения и ядра.
- Рекомендуется выстраивать физическую топологию сети по типу расширенной звезды от центрального здания до всех остальных зданий в рамках одного комплекса.



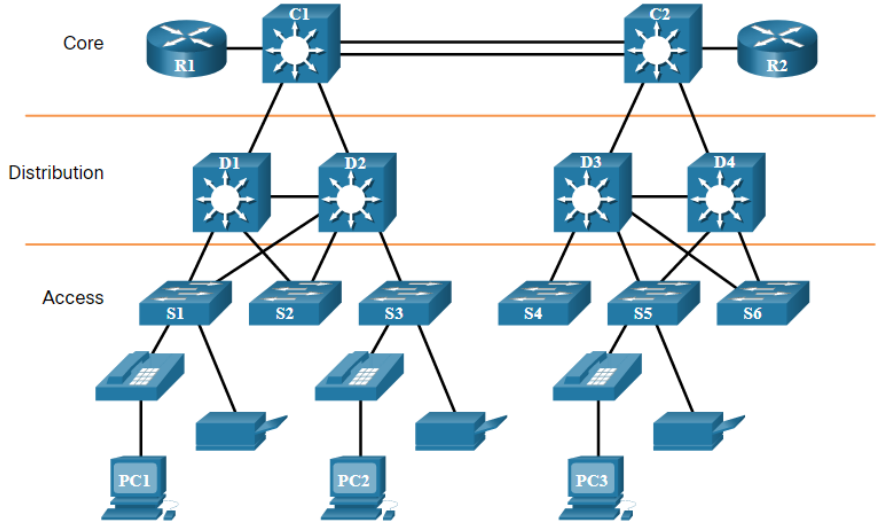
Двухуровневая сеть кампуса

- Используется, когда не требуются отдельные уровни распределения и ядра.
- Подходит для небольших кампусов, или для кампусов, состоящих из одного здания.
- Также известен как *свернутая конструкция основной* сети.



Роль коммутируемых сетей

- Сети в корне изменились с плоской сети концентраторов на коммутируемые локальные сети в иерархической сети.
- Коммутируемая локальная сеть обеспечивает дополнительную гибкость, управление трафиком, качество обслуживания и безопасность.
- Коммутируемая локальная сеть может также поддерживать беспроводные сети и другие технологии, такие как IP-телефонии и услуги мобильной связи.



11.2 Масштабируемые сети

Проектирование масштабируемости

Масштабируемость — это термин для сети, которая может расти без потери доступности и надежности.

Разработчик сети должен разработать стратегию, чтобы сеть была доступна и масштабируема эффективно и легко.

Это обеспечивается следующими способами:

- Резервирование
- Несколько каналов связи
- Масштабируемый протокол маршрутизации
- Беспроводное соединение

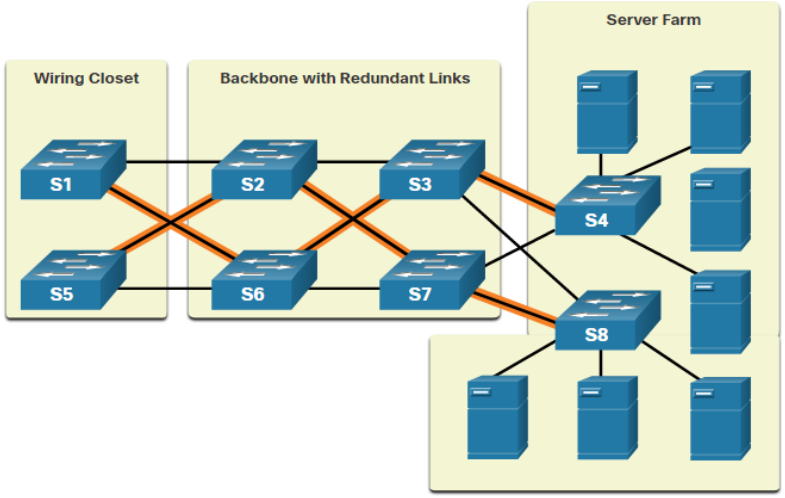
Планирование резервирования

Резервирование защищает от перебоев в работе всех сетевых служб в случае отказа в отдельной точке.

- Установка дублирующего оборудования
- Предоставление услуг аварийного переключения для критически важных устройств

Резервные пути предоставляют альтернативные физические маршруты передачи данных по сети.

- Тем не менее избыточные маршруты в коммутируемой сети Ethernet могут привести к возникновению логических петель 2-го уровня.
- По этой причине необходимо использовать протокол STP.



Уменьшение размера домена сбоев

Хорошо продуманная сеть контролирует трафик и ограничивает размер доменов сбоев.

- В иерархической модели проектирования домены сбоев заканчиваются на уровне распределения.
- Каждый маршрутизатор выступает в качестве шлюза для ограниченного количества пользователей уровня доступа.

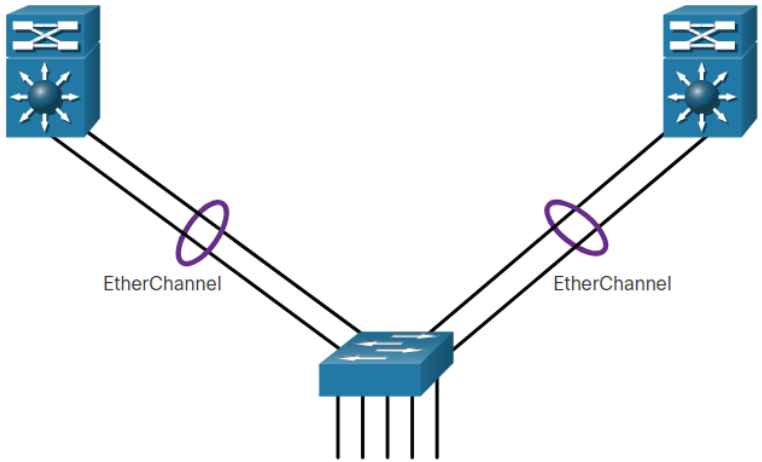
Маршрутизаторы или многоуровневые коммутаторы обычно развертываются парами в конфигурации, называемой блоком коммутатора здания или подразделения.

- Каждый блок коммутации функционирует независимо от других.
- Поэтому в случае отказа отдельного устройства не будет сбоя всей сети.

Увеличение пропускной способности

Агрегация каналов, например EtherChannel, позволяет администратору увеличить пропускную способность между устройствами за счет создания единого логического канала, состоящего из нескольких физических каналов.

- EtherChannel объединяет существующие порты коммутатора в один логический канал с помощью интерфейса канала порта.
- Большинство задач по настройке выполняются на интерфейсе Port Channel (а не на каждом отдельном порту), чтобы обеспечить согласованность конфигурации каналов.
- EtherChannel может балансировать нагрузку между каналами.



Расширение уровеня доступа

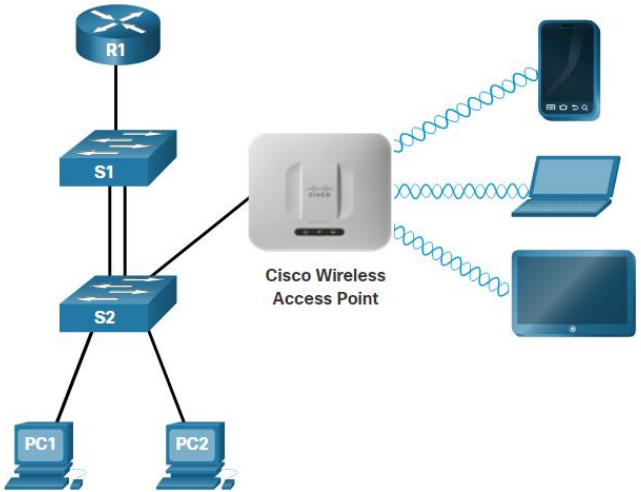
Все более важное значение приобретает расширение возможностей подключения на уровне доступа посредством беспроводного подключения.

- Беспроводное подключение на уровне доступа обеспечивает повышенную гибкость, сокращение затрат и возможность масштабирования и адаптации к изменяющимся требованиям бизнеса.

  - Для беспроводной связи конечным устройствам требуется беспроводная сетевая плата для подключения к беспроводному маршрутизатору или точке беспроводного доступа (AP).

При внедрении беспроводной сети следует учитывать следующие факторы:

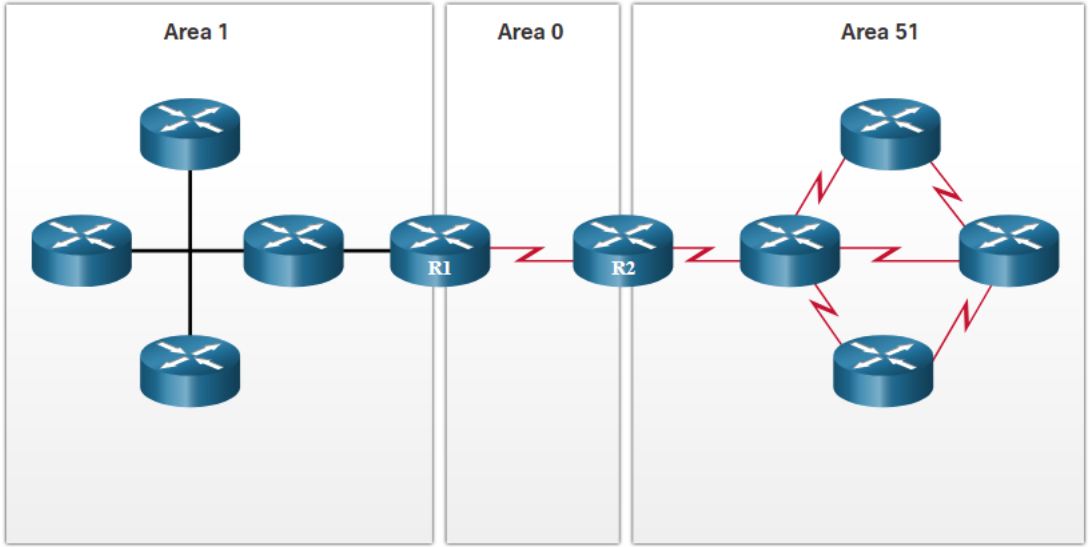
- Типы беспроводных устройств, подключенных к WLAN
- Требования к беспроводному покрытию
- Вопросы защиты от помех
- Вопросы безопасности



Протоколы маршрутизации

Усовершенствованные протоколы маршрутизации, например OSPF, используются в крупных сетях.

- OSPF — это протокол маршрутизации состояния канала, который использует области для поддержки иерархических сетей.
- Маршрутизаторы OSPF устанавливают и поддерживают отношения смежности с другими маршрутизаторами OSPF, подключенными к сети.
- Маршрутизаторы OSPF синхронизируют свою базу данных состояния канала.
- При изменении сети отправляются обновления состояния канала, информирующие другие маршрутизаторы OSPF об изменении и установлении нового оптимального пути, если он доступен.




CISCO

Заполните, пожалуйста,
опрос о занятии по ссылке в чате

До новых встреч!
Приходите на следующие занятия