Обслуживание сети

Занятие десятое

Cisco | Networking Academy®
Mind Wide Open™

Ознакомившись с этой главой, вы научитесь:

- определять устройства и протоколы, используемые в небольших сетях;
- объяснять, как небольшая сеть может стать основой для более обширных сетей;
- описывать потребность в основных мерах по обеспечению безопасности сетевых устройств;
- определять уязвимости в системе сетевой безопасности и основные методы подавления последствий, вызванных подобными нарушениями;
- выполнять настройку параметров сетевых устройств с помощью соответствующих защитных функций, чтобы минимизировать последствия, вызванные нарушениями сетевой безопасности;
- использовать выходные данные команд **`ping`** и **`tracert`** для достижения относительной производительности сети;
- использовать основные команды **`show`** для проверки параметров конфигурации и состояния интерфейса устройства;
- использовать основные команды узла и системы IOS для получения сведений об устройствах в сети;
- объяснять принципы работы файловых систем на маршрутизаторах и коммутаторах;
- применять команды для резервного копирования и восстановления файла конфигурации IOS.

Направления деятельности

Обслуживание

Обеспечение безопасности

Диагностика

Устранение неисправностей

Документация

- **Сетевая документация** — физическая и логическая топология
- **Реестр устройств** — список устройств, использующих или образующих сеть
- **Бюджет** — детализированный бюджет ИТ, включая бюджет на закупку оборудования на финансовый год.
- **Анализ трафика** — необходимость документирования протоколов, приложений и служб, а также соответствующих им требований к трафику.

Факторы выбора оборудования

COST

PORTS

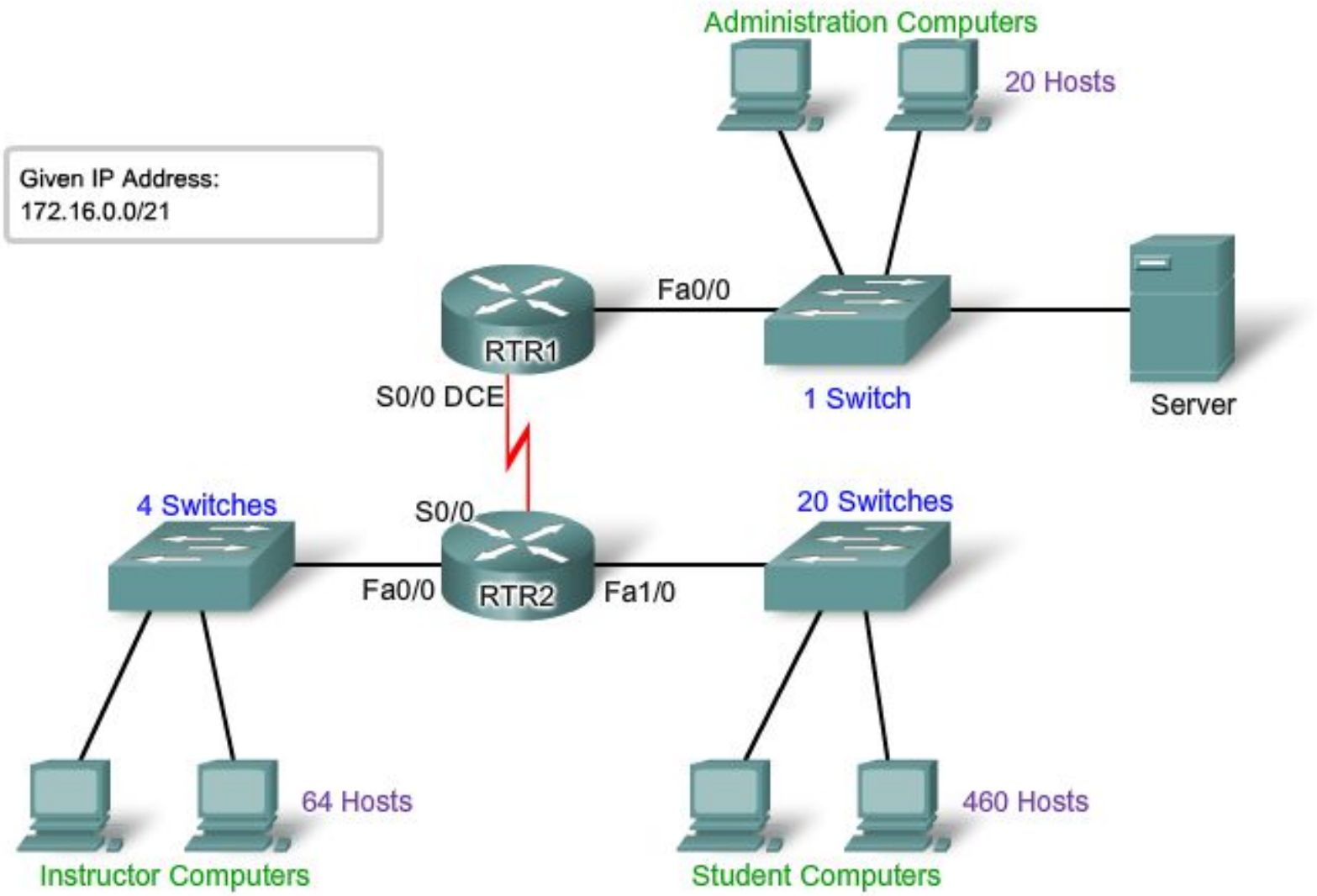
SPEED

EXPANDABLE/ MODULAR

MANAGEABLE

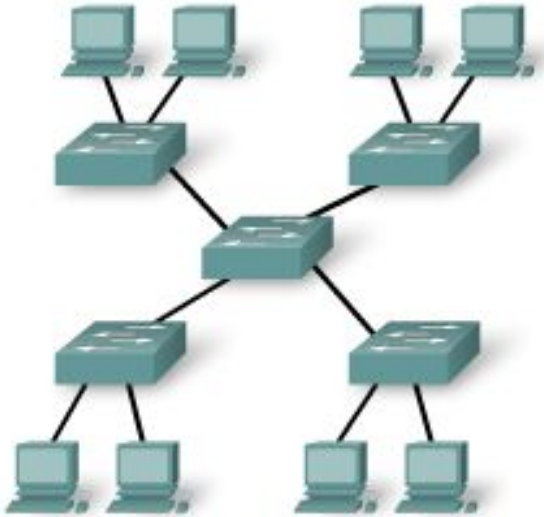
"cost per port"

Планирование пространства IP-адресов

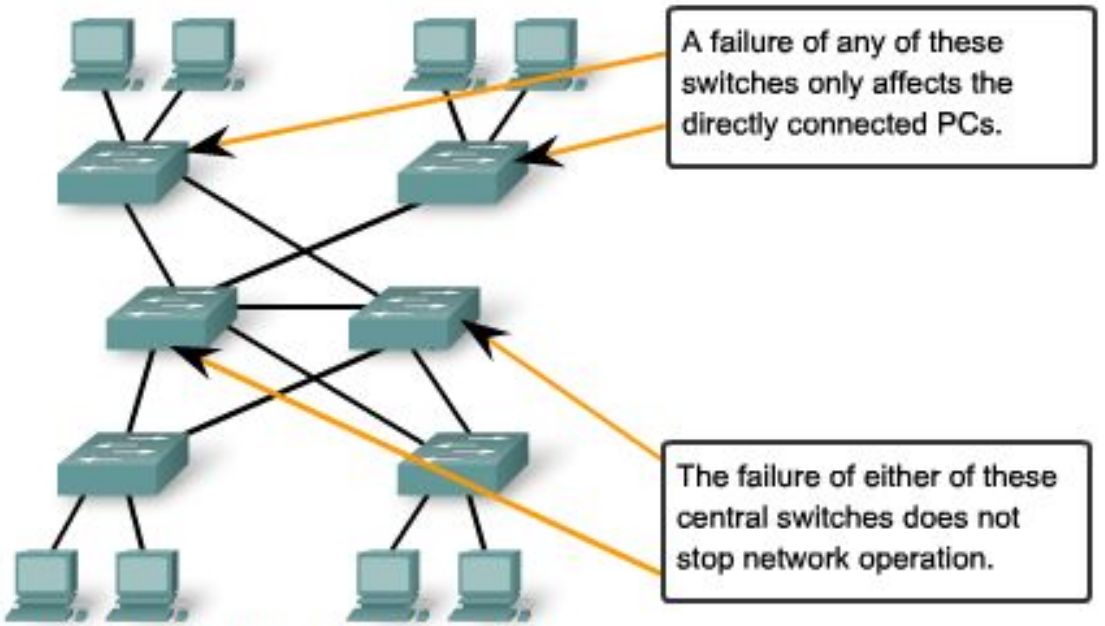


Резервирование

One large, central switch

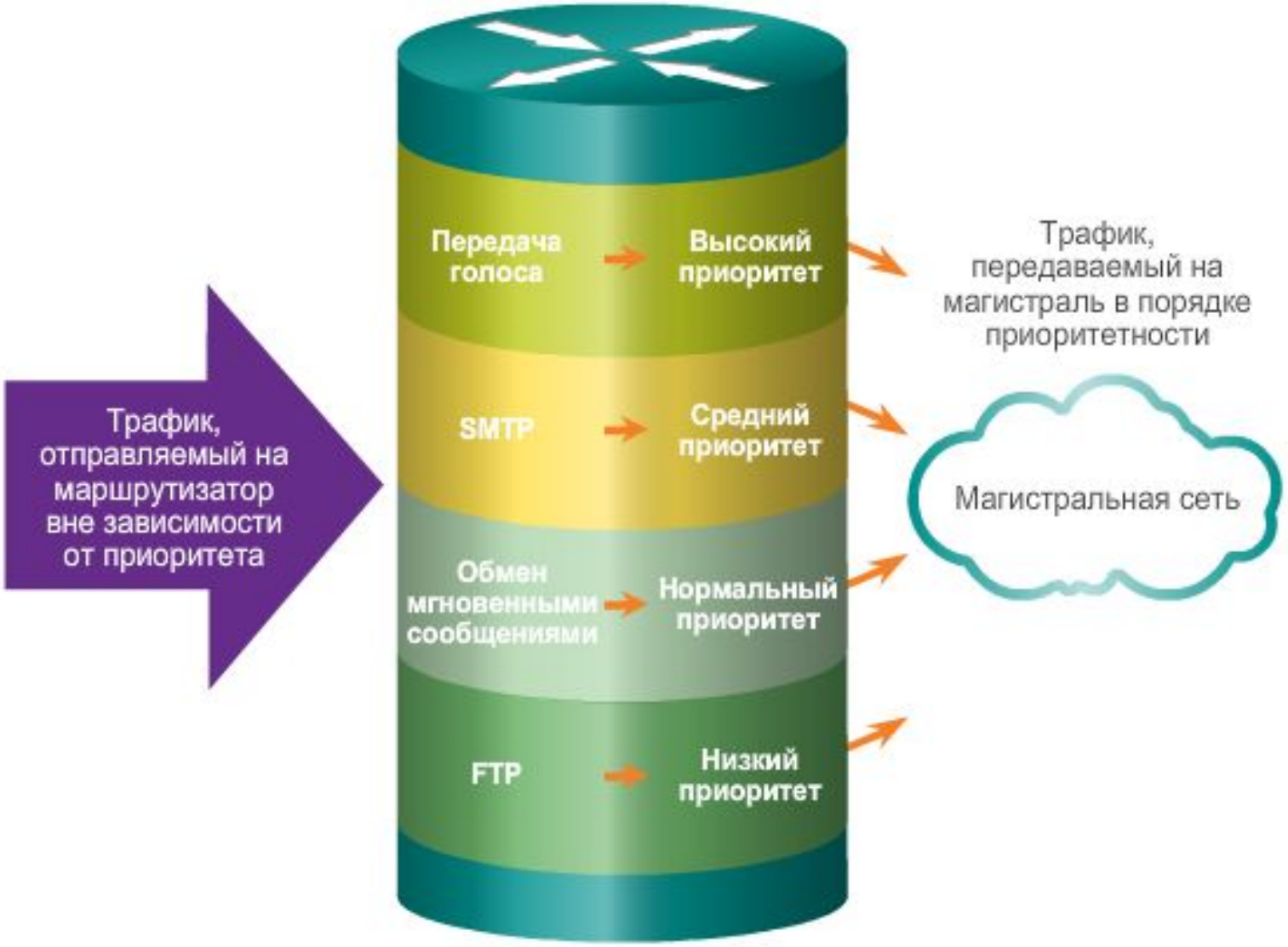


Multiple switches, connected with a central switch

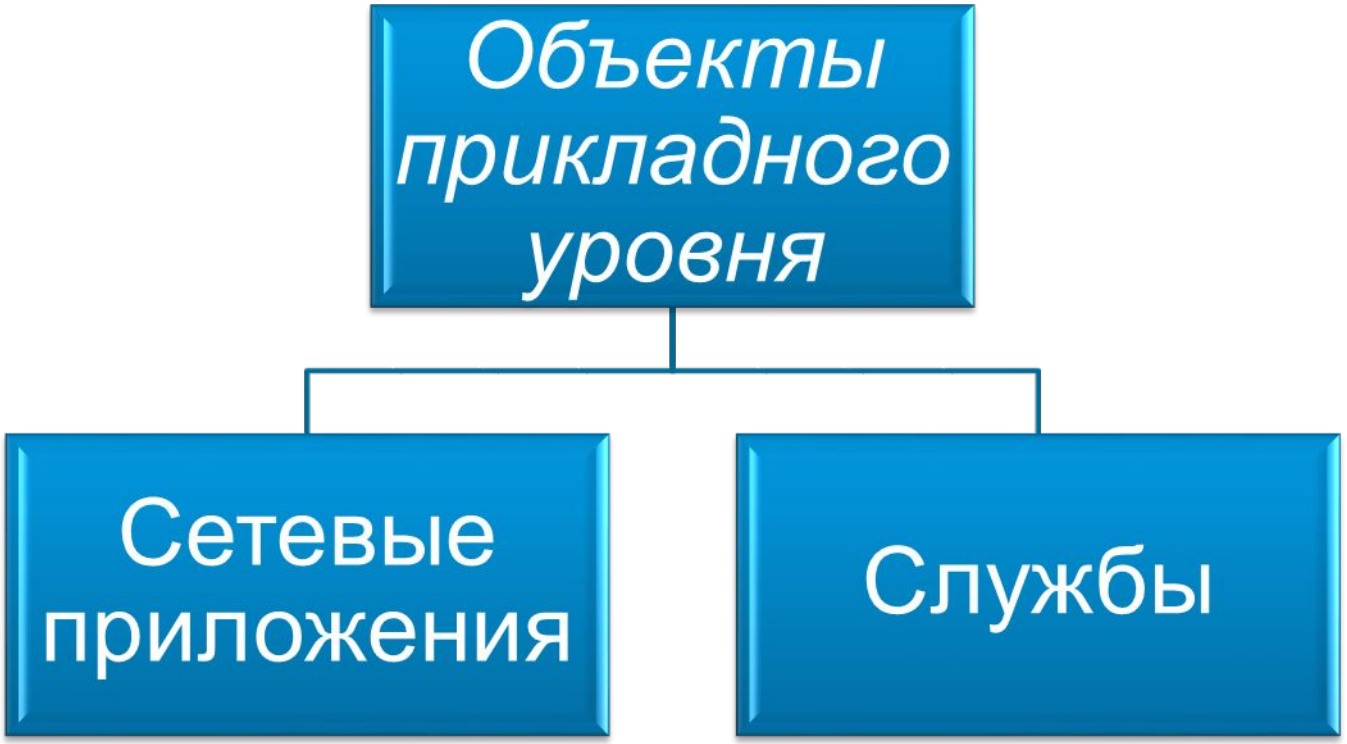


Two central switches with redundancy

Учет приоритезации

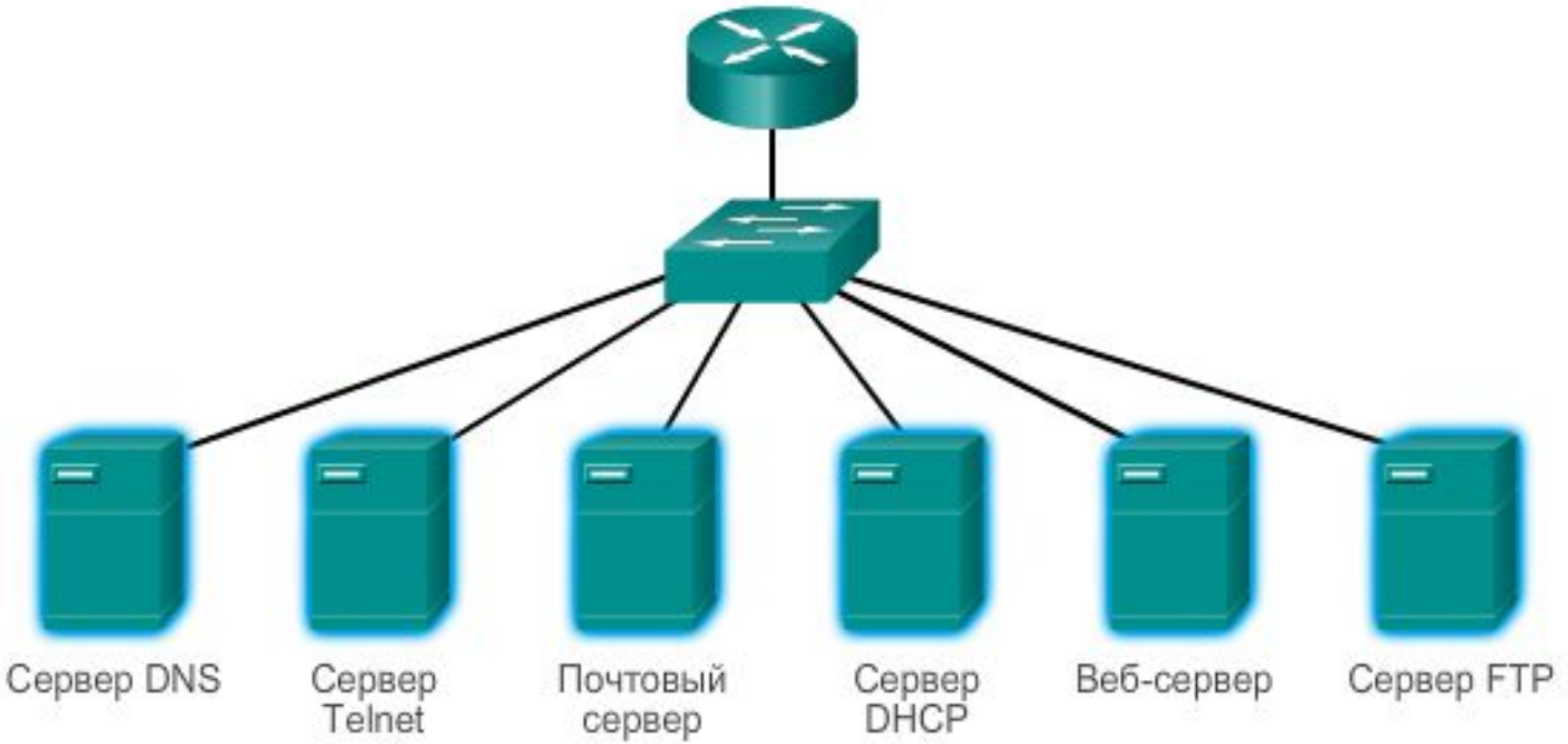


Виды приложений



Полезность сети определяется полезностью используемых в ней приложений!

Примеры служб

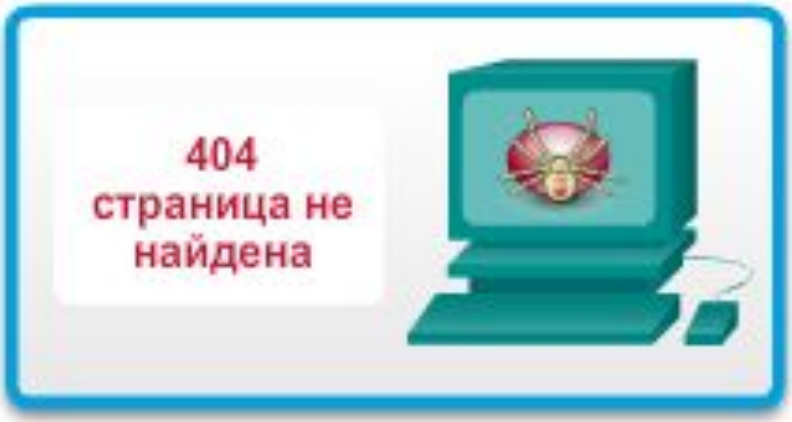


Угрозы безопасности

Хищение информации

Потеря данных и манипуляции с данными

Кража личной информации

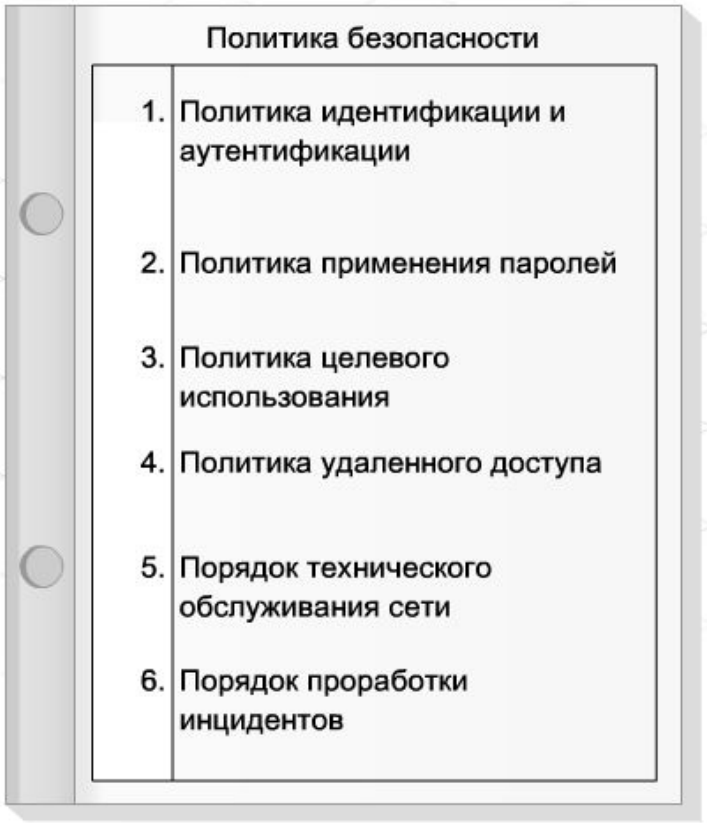


Прекращение обслуживания

Классы физических угроз сети

- Эксплуатационные угрозы
- Угрозы окружающей среды
- Угрозы электропитания
- Угрозы механических конструкций

Политика безопасности – формальное изложение правил, которых должны придерживаться пользователи при доступе к технологическим и информационным ресурсам.



ISO/IEC 27002
12 секций

Уязвимости

Технологические

Конфигурационные

Политики безопасности

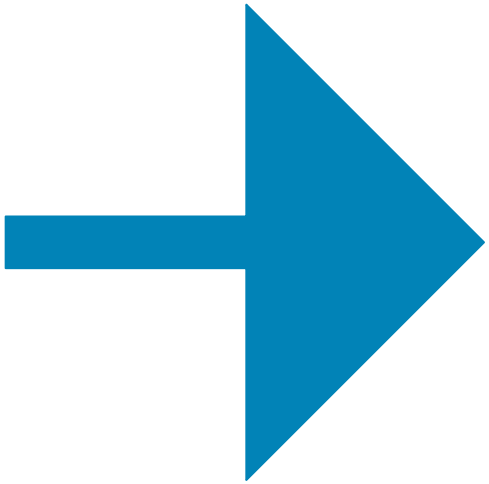
Атаки с использованием зловредного кода (Malicious Code Attacks)

Вирус – программа, которая функционирует и распространяется путем изменения других программ и файлов. Вирус не запускается сам – он должен быть активирован.

Червь аналогичен вирусу с тем отличием, что ему не требуется внедряться в существующую программу. Червь рассылает копии самого себя по сети на все подключенные узлы.

"Троянским конем" называют не размножающуюся программу, представляющую собой инструмент для атаки, замаскированный под некоторую легитимную программу.

Разведка в КС (Reconnaissance)



Internet queries

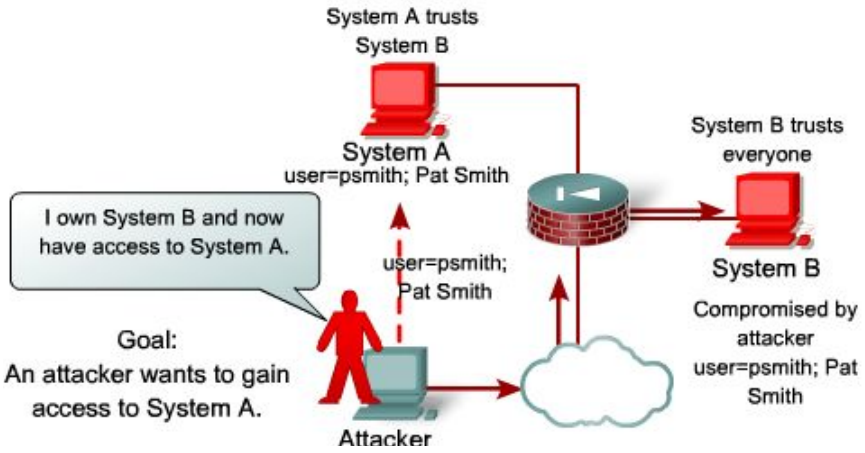
Ping sweeps

Port scans

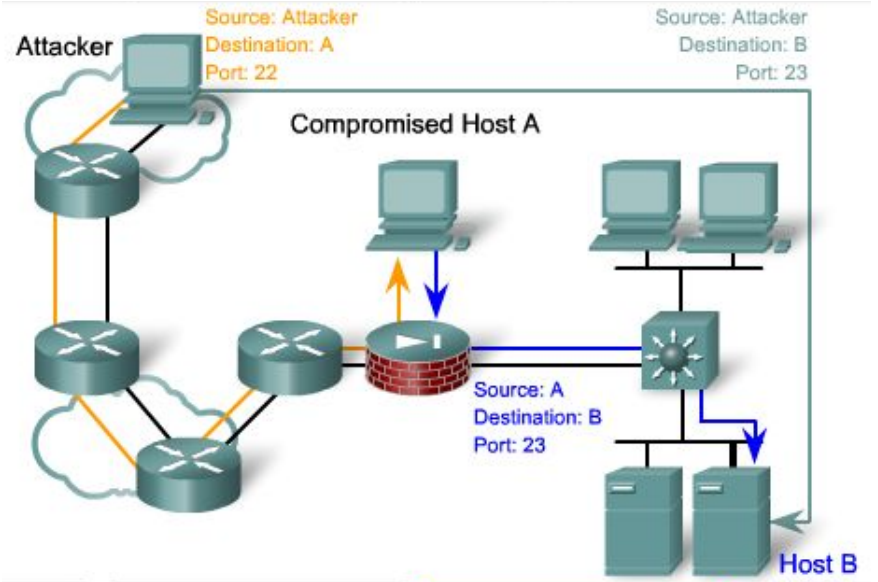
Packet sniffers

Атаки на получение доступа

Trust Exploitation

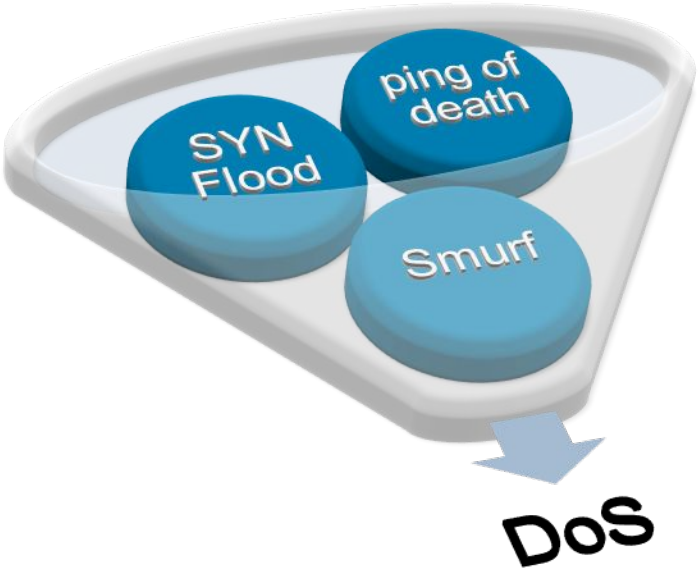


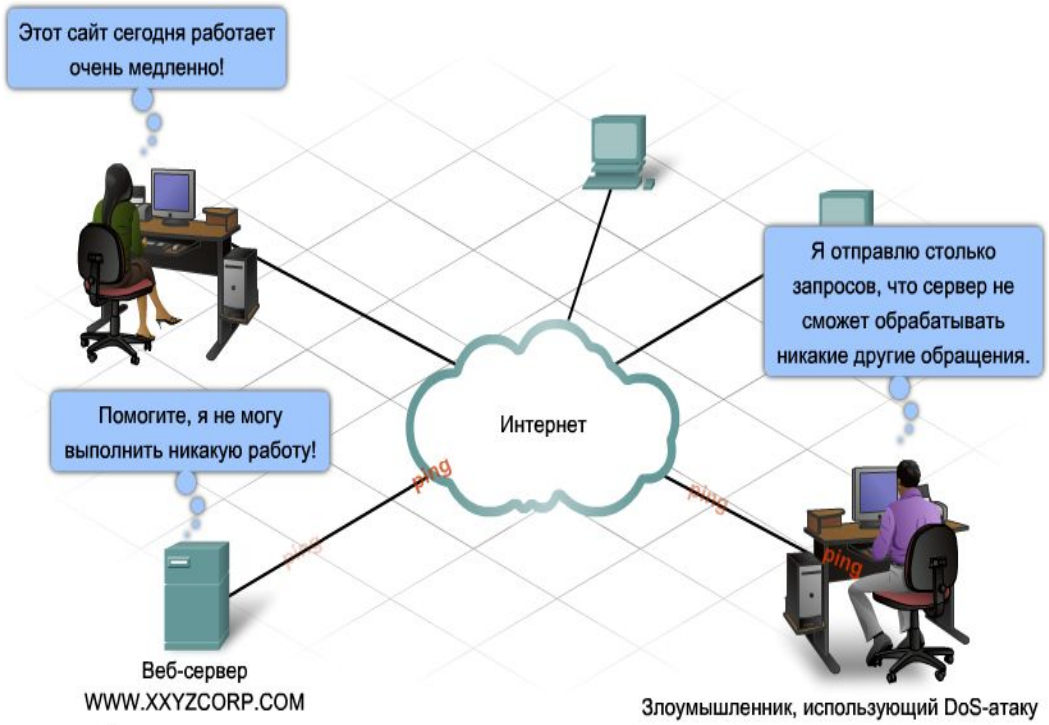
Port Redirection



Man-in-the-Middle

Виды DoS (denial of services) атак





Методы противодействия атакам

Резервное копирование

Использование антивируса

Установка обновлений

AAA

Устройства защиты Cisco

Серверные межсетевые экраны

Беспроводные маршрутизаторы Linksys с интегрированным межсетевым экраном

Персональный межсетевой экран

Cisco Discovery Protocol (CDP) – протокол второго уровня

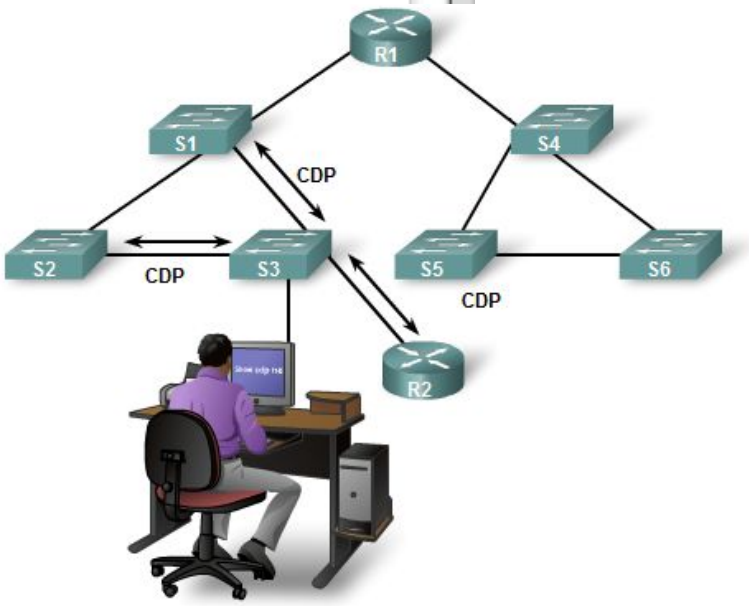
```
R3#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S3               Fas 0/0             151         S I       WS-C2950  Fas 0/6
R2               Ser 0/0/1           125          R        1841      Ser 0/0/1

R3#show cdp neighbors detail

Device ID: R2
Entry address(es):
  IP address : 192.168.1.2
Platform: Cisco 1841,  Capabilities: Router Switch IGMP
Interface: Serial0/0/1,  Port ID (outgoing port): Serial0/0/1
Holdtime : 161 sec

Version :
```




```
!To disable CDP globally use...
R3(config)#no cdp run
!
!or, to disable CDP on only an interface...
R3(config-if)#no cdp enable
```

Получение информации об интерфейсах маршрутизатора

```
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES manual administratively down down
Serial0/0/0                unassigned      YES unset  administratively down down
FastEthernet0/1            unassigned      YES unset  administratively down down
Serial0/0/1                unassigned      YES unset  administratively down down
```

```
R1#show interfaces
FastEthernet0/0 is administratively down, line protocol is down
  Hardware is AmdFE, address is 000c.3010.9260 (bia 000c.3010.9260)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

Использование MAC и ARP

```
R1#show interfaces fastethernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 000c.3010.9260 (bia 000c.3010.9260)
  Internet address is 172.16.3.1/24
  <output omitted>
R1#
```

```
R1#show interfaces serial 0/0/0
Serial0/0/0 is down, line protocol is down
  Hardware is PowerQUICC Serial
  Internet address is 172.16.2.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
<output omitted>
```

Настройка SSH

```
router# hostname cisco
cisco# clock set 17:10:00 28 Aug 2009
cisco# configure terminal
cisco(config)# ip domain name test.dom
cisco(config)# crypto key generate rsa
cisco(config)# service password-encryption
cisco(config)# username user password 7 Pa$$w0rd
cisco(config)# line vty 0 4
cisco(config-line)# transport input ssh
cisco(config-line)# logging synchronous
cisco(config-line)# exec-timeout 60 0
cisco(config-line)# exit
cisco(config)# exit
```

Устанавливаем точное время для генерации ключа
Входим в режим конфигурирования
Указываем имя домена (необходимо для генерации ключа)
Генерируем RSA ключ
Активируем шифрование паролей в конфигурационном файле
Заводим пользователя с именем user, паролем Pa$$w0rd
Указываем средой доступа через сеть по умолчанию SSH
Указываем время таймаута до автоматического закрытия SSH сессии в 60 минут

Файловая система Cisco IFS

```
Router#show file systems
File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
             -             -    opaque     rw   null:
             -             -   network     rw   tftp:
*    256487424     183234560      disk     rw   flash0: flash:#
             -             -      disk     rw   flash1:
        262136        254779     nvram     rw   nvram:
             -             -    opaque     wo   syslog:
             -             -    opaque     rw   xmodem:
             -             -    opaque     rw   ymodem:
             -             -   network     rw   rcp:
             -             -   network     rw   http:
             -             -   network     rw   ftp:
             -             -   network
             -             -    opaque
             -             -   network
             -             -    opaque
```

```
Router#cd nvram:
Router#pwd
nvram:/
Router#dir
Directory of nvram:/

  253  -rw-        1156      <no date>  startup-config
  254  ----           5      <no date>  private-config
```

Резервное копирование конфигурации

```
Router#copy running-config tftp
Remote host []? 131.108.2.155
Name of configuration file to write[tokyo-config]?tokyo.2
Write file tokyo.2 to 131.108.2.155? [confirm]
Writing tokyo.2 !!!!!! [OK]
```

```
R1#copy running-config usbflash0:
Destination filename [running-config]? R1-Config
5024 bytes copied in 0.736 secs (6826 bytes/sec)
```