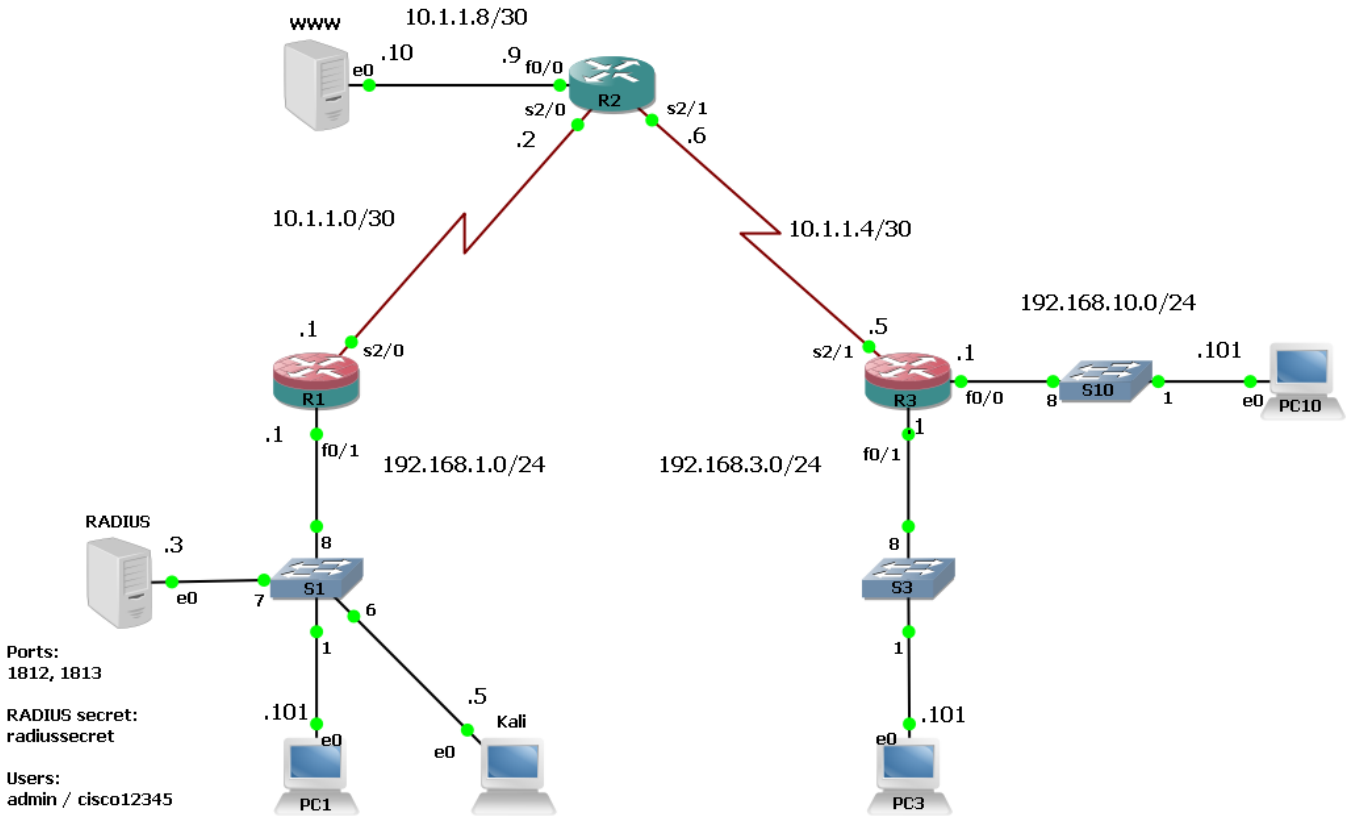
CCNA Security

Лабораторная работа 11

Изучение протокола OSPFv2

Топология



Описание

В этой лабораторной работе вы обеспечите дополнительную безопасность в протоколе OSPFv2: настроите пассивные интерфейсы и внедрите аутентификацию.

Таблица адресации

Устройство	Интерфейс	IPv4-адрес/Маска подсети	Шлюз по умолчанию	Описание
R1	Fa0/1	192.168.1.1/24	-	LAN interface
	Se2/0	10.1.1.1/30	-	WAN interface (To R2)
R2	Se2/0	10.1.1.2/30	-	To R1
	Se2/1	10.1.1.6/30	-	To R3
	Fa0/0	10.1.1.9/30	-	To WWW server
R3	Fa0/1	192.168.3.1/24	-	LAN interface
	Fa0/0	192.168.10.1/24	-	Conference Room
	Se2/1	10.1.1.5/30	-	WAN interface (To R2)
PC1	NIC	192.168.1.101/24	192.168.1.1	-
PC2	NIC	192.168.3.101/24	192.168.3.1	-
PC10	NIC	192.168.10.101/24	192.168.10.1	-
Kali	NIC	192.168.1.5/24	192.168.1.1	-
RADIUS	NIC	192.168.1.3/24	192.168.1.1	-
WWW	NIC	10.1.1.10/24	10.1.1.9	-

Имена пользователей и пароли

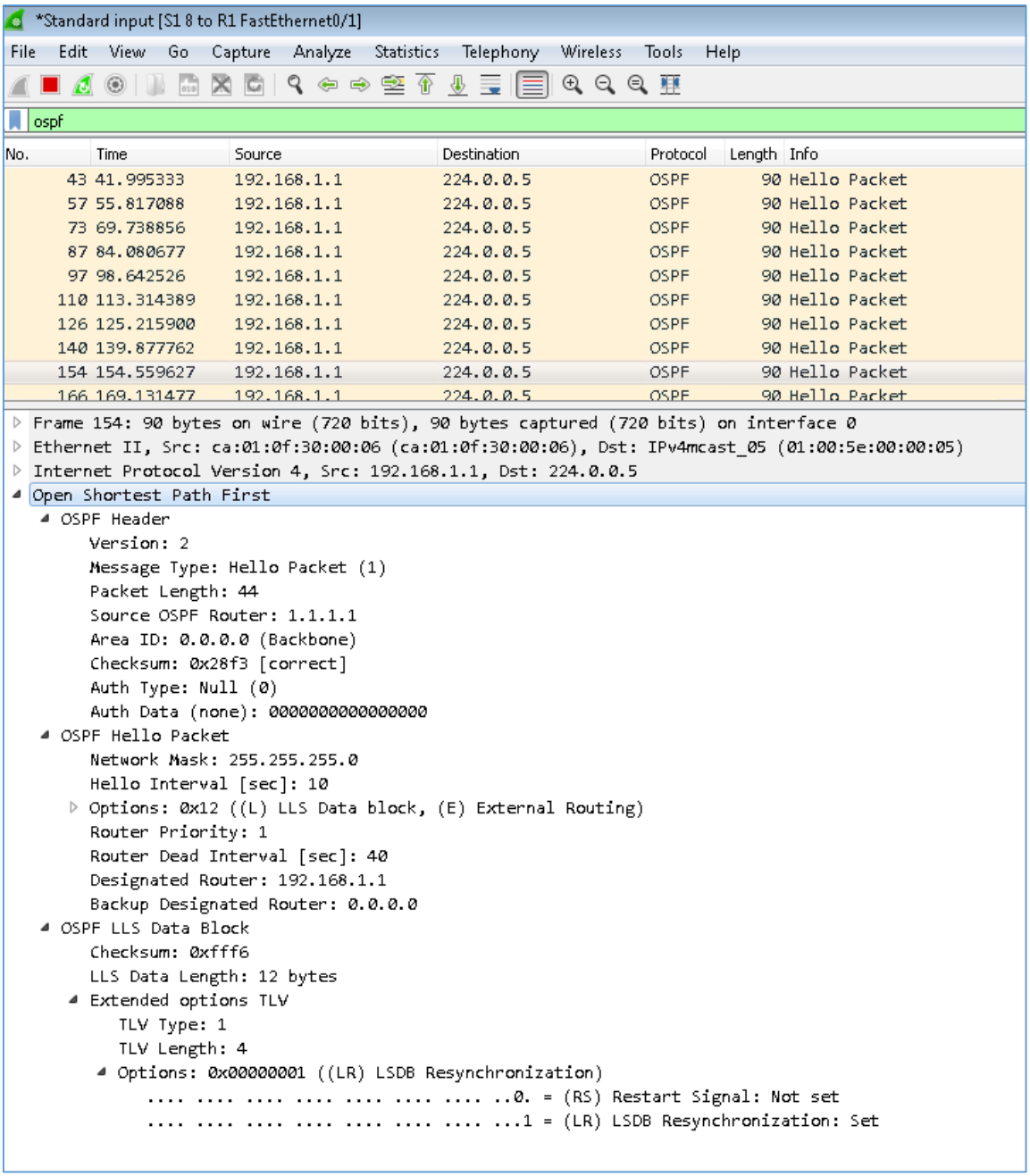
	Console		VTY		Enable
Устройство	Имя пользователя	Пароль	Имя пользователя	Пароль	Пароль
R1	admin	cisco12345	admin	cisco12345	cisco12345
R2	-	-	-	-	-
R3	admin	cisco12345	admin	cisco12345	cisco12345

Устройство	Имя пользователя	Пароль
PC1	Student1	1
PC2	Student1	1
PC10	Student1	1
Kali	root	toor

Часть 1: Изучение протокола OSPFv2

1. Запустите захват на линке между R1 и S1. Для этого в окне GNS3 щёлкните правой кнопкой мыши по линку между R1 и S1, в контекстном меню выберите **Start Capture**. В открывшемся окне просто нажмите **OK**. Дождитесь открытия Wireshark.

2. Введите в поле Display Filter слово **ospf** и нажмите Enter. Интерфейс fa0/1 участвует в процессе OSPF, поэтому раз в 10 секунд по умолчанию маршрутизатор будет высылать с этого интерфейса Hello-пакеты, а приходящие Hello-пакеты будут обрабатываться. Это не очень хорошо с точки зрения производительности (лишний ненужный траффик) и безопасности (злоумышленник может сдружиться с вашим маршрутизатором и подсунуть «левую» маршрутную информацию). Все параметры маршрутизатора в контексте протокола OSPF можно увидеть в Hello-пакете (Router ID, номер и тип области, таймеры, IP-адрес и маску на интерфейсе, тип аутентификации).



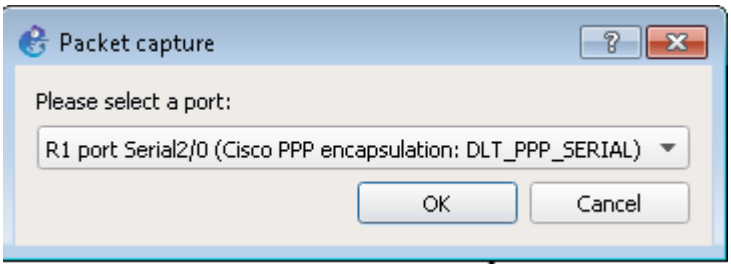
3. Перейдите в консоль маршрутизатора R1.

4. Войдите в режим конфигурирования.
```
R1# conf t
```

5. Сделайте все интерфейсы пассивными, кроме интерфейса, смотрящего в сторону провайдера.
```
R1(config)# router ospf 1
R1(config-router)# passive-interface default
R1(config-router)# no passive-interface s2/0
R1(config-router)# exit

R1(config)# do show ip proto
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Routing on Interfaces Configured Explicitly (Area 0):
    Serial2/0
    FastEthernet0/1
  Passive Interface(s):
    FastEthernet0/0
    FastEthernet0/1
    FastEthernet1/0
    FastEthernet1/1
    Serial2/1
    Serial2/2
    Serial2/3
    VoIP-Null0
< Вывод опущен >

R1(config)# do show ip ospf int fa0/1
FastEthernet0/1 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Interface Enable
  Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  < Вывод опущен >
```

6. Вернитесь в Wireshark на основной машине. Посмотрите, перестанут ли приходит новые пакеты Hello-пакеты? После наблюдений закройте основное окно Wireshark.

7. Запустите захват на линке между R1 и R2. Для этого в окне GNS3 щёлкните правой кнопкой мыши по линку между R1 и R2, в контекстном меню выберите **Start Capture**. В открывшемся окне выберите **R1 port Serial2/0 (Cisco PPP encapsulation: DLT_PPP_Serial)** и нажмите **OK**. Дождитесь открытия Wireshark.



8. Введите в поле Display Filter слово **ospf** и нажмите Enter.

9. Вернитесь в консоль маршрутизатора R1. В целях дополнительной защиты настройте аутентификацию OSPF на интерфейсе s2/0.

```
R1(config)# int s2/0
R1(config-if)# ip ospf message-digest-key 1 md5 ospfpass
R1(config-if)# ip ospf authentication message-digest

R1(config-if)# do show ip ospf int s2/0
Serial2/0 is up, line protocol is up
  Internet Address 10.1.1.1/30, Area 0, Attached via Interface Enable
  Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 781
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           781       no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

10. Через некоторое время соседство между R1 и R2 порвётся, т.к. более у них не совпадают тип аутентификации и данные аутентификации.

```
%OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial2/0 from FULL to DOWN, Neighbor
Down: Dead timer expired
```

11. Вернитесь в Wireshark на основной машине. Выберите любой из последних пакетов OSPF от 10.1.1.1 (для простоты можно применить фильтр **ospf and ip.src == 10.1.1.1**). Обратите внимание на изменившееся поле Auth Type и наличие некоторых других дополнительных параметров. Можно ли тут разобрать ключ? После наблюдений закройте основное окно Wireshark.

```
Auth Type: Cryptographic (2)
Auth Crypt Key id: 1
Auth Crypt Data Length: 16
Auth Crypt Sequence Number: 1601367041
Auth Crypt Data: 61f583a5d420bf4bde092342348b0128
```

12. Подключитесь к консоли маршрутизатора R2, настройте аналогичные параметры аутентификации на интерфейсах s2/0 и s2/1. Через некоторое время соседство между R1 и R2 восстановится, а между R2 и R3 порвётся.

```
R2# conf t
R2(config)# int s2/0
R2(config-if)# ip ospf message-digest-key 1 md5 ospfpass
R2(config-if)# ip ospf authentication message-digest
R2(config-if)# exit
R2(config)# int s2/1
R2(config-if)# ip ospf message-digest-key 1 md5 ospfpass
R2(config-if)# ip ospf authentication message-digest
R2(config-if)# end

%OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial2/0 from LOADING to FULL, Loading
Done
%OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial2/1 from FULL to DOWN, Neighbor
Down: Dead timer expired
```

13. Подключитесь к консоли маршрутизатора R3. Сделайте все интерфейсы пассивными, кроме интерфейса, смотрящего в сторону провайдера. Настройте аутентификацию на интерфейсе s2/1. Через некоторое время соседство между R2 и R3 восстановится.

```
R3# conf t
R3(config)# router ospf 1
R3(config-router)# passive-interface default
R3(config-router)# no passive-interface s2/1
R3(config-router)# exit
R3(config)# int s2/1
R3(config-if)# ip ospf message-digest-key 1 md5 ospfpass
R3(config-if)# ip ospf authentication message-digest
R3(config-if)# end

%OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial2/1 from LOADING to FULL, Loading
Done

R3# show ip proto
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Routing on Interfaces Configured Explicitly (Area 0):
    Serial2/1
    FastEthernet0/0
    FastEthernet0/1
  Passive Interface(s):
    FastEthernet0/0
    FastEthernet0/1
    FastEthernet1/0
```

```
    FastEthernet1/1
    Serial2/0
    Serial2/2
    Serial2/3
    VoIP-Null0
  < Вывод опущен >
R3# show ip ospf int s2/1
Serial2/1 is up, line protocol is up
  Internet Address 10.1.1.5/30, Area 0, Attached via Interface Enable
  Process ID 1, Router ID 3.3.3.3, Network Type POINT_TO_POINT, Cost: 781
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           781       no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:04
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1

R3# show ip ospf nei
Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   FULL/  -        00:00:36    10.1.1.6        Serial2/1
```