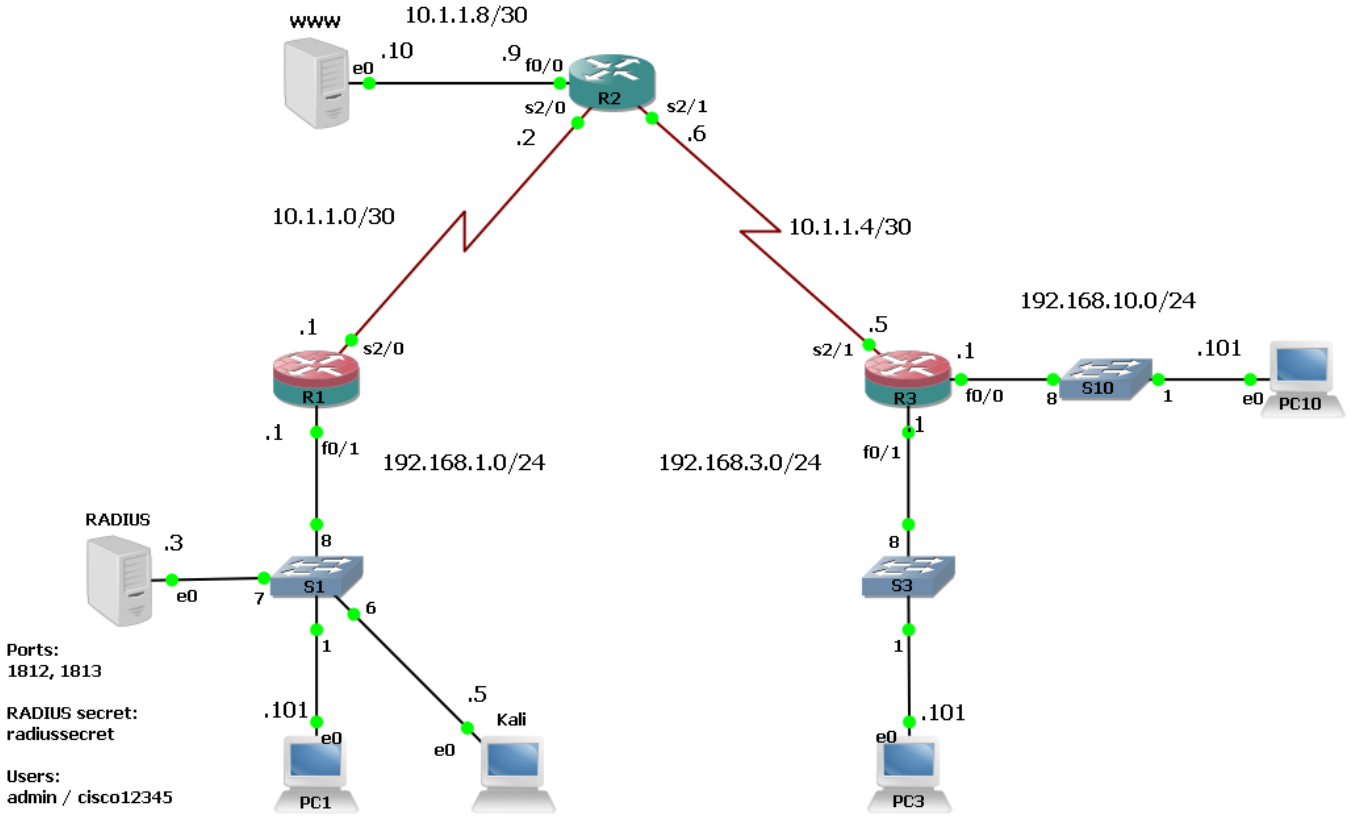
CCNA Security

Лабораторная работа 10

Изучение протокола CDP

Топология



Описание

В этой лабораторной работе вы примерите на себя роль злоумышленника, ставшего человеком посредине (Man-In-The-Middle, MITM). С помощью сниффера Wireshark вы будете отлавливать пакеты, а затем их анализировать. В ходе анализа вы убедитесь в некоторой небезопасности протокола CDP, а затем отключите его. Открытый протокол LLDP работает похожим образом, рекомендации к его использованию такие же, однако на лабораторном оборудовании протокол LLDP не поддерживается.

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 CDP

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. Подключитесь к консоли маршрутизатора R1.

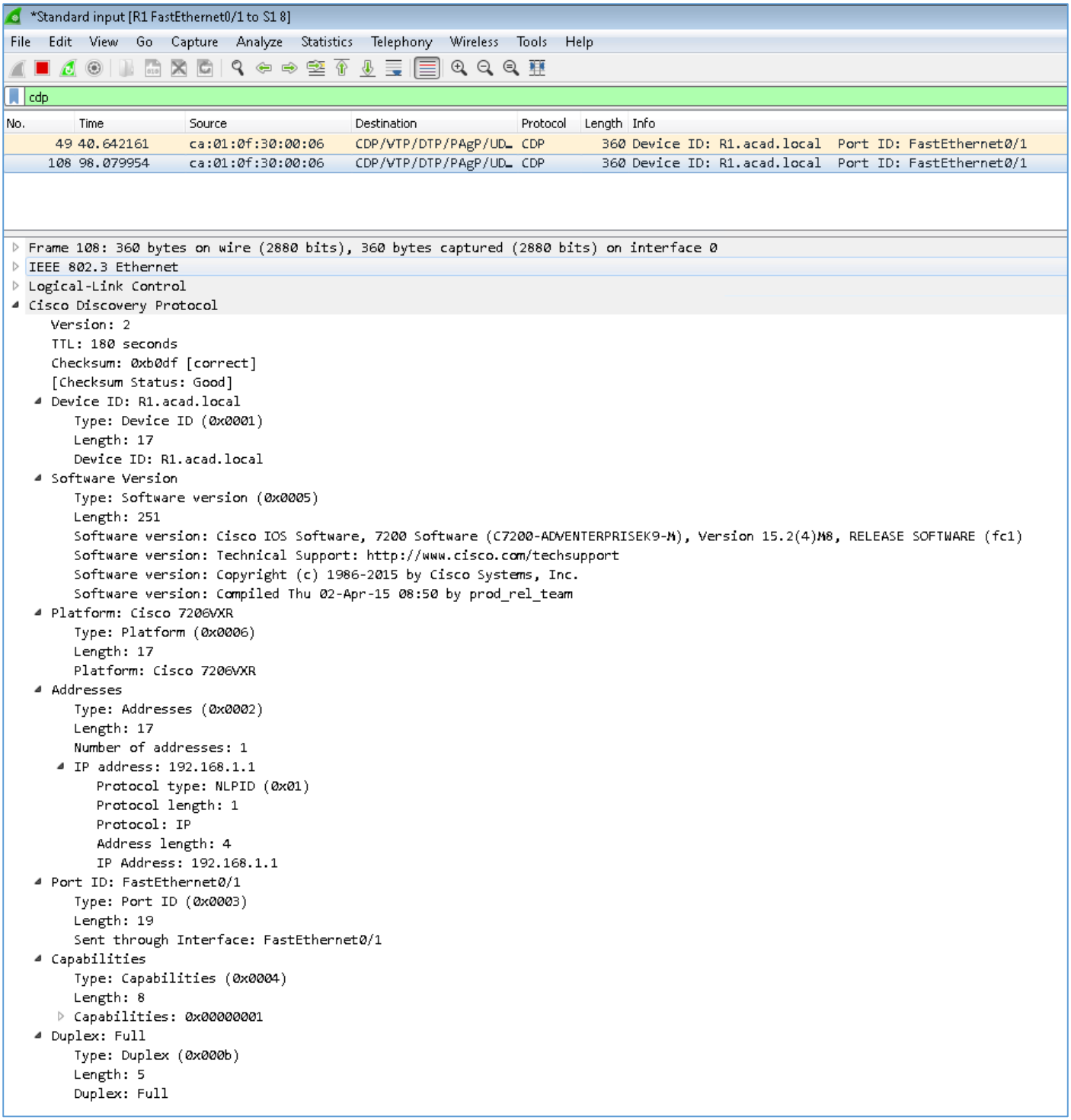
3. На маршрутизаторах и коммутатора протокол CDP включен по умолчанию, устройство будет отправлять основную информацию о себе со всех включённых портов раз в 60 секунд. Проверьте это.

```
R1# show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is  enabled

R1# show cdp interface
FastEthernet0/0 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
FastEthernet0/1 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
FastEthernet1/0 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
FastEthernet1/1 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial2/0 is up, line protocol is up
  Encapsulation PPP
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
< Вывод опущен >
```

4. Вернитесь в Wireshark на основной машине.

5. Введите в поле Display Filter слово **cdp** и нажмите Enter. Выберите любой пакет из представленных и изучите его содержимое. Найдите имя устройства, модель устройства, версию IOS, IP-адрес для управления.



6. Вернитесь в консоль маршрутизатора R1. Отключите CDP глобально.

```
R1# conf t
R1(config)# no cdp run
R1(config)# end
R1# show cdp
% CDP is not enabled

R1# show cdp interface
% CDP is not enabled
```

7. Вернитесь в Wireshark на основной машине. Посмотрите, перестанут ли приходит новые пакеты протокола CDP? После наблюдений закройте основное окно Wireshark.

Часть 2: Отключение протокола CDP на маршрутизаторе R3

1. Подключитесь к консоли маршрутизатора R3.

2. Отключите CDP глобально.

```
R3# conf t
R3(config)# no cdp run
R3(config)# end

R3# show cdp
% CDP is not enabled

R3# show cdp interface
% CDP is not enabled
```