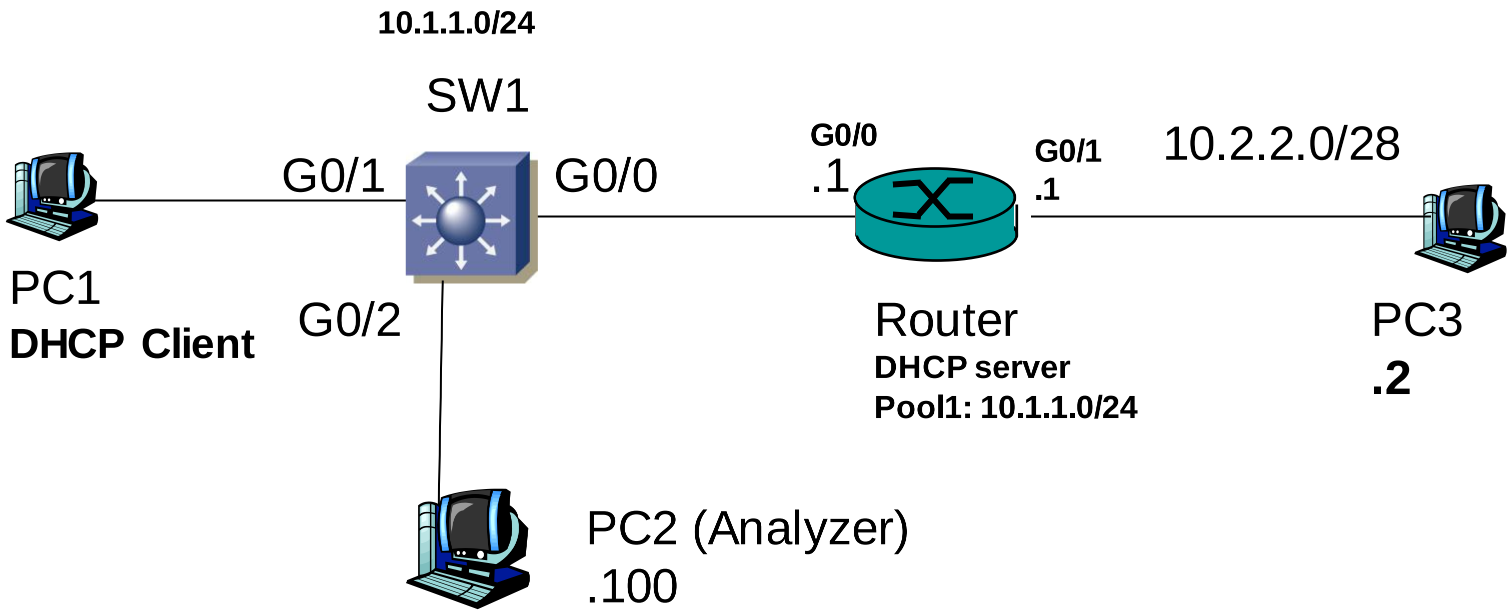
Figure 1



Lab – Mitigating data plane attacks by using ACL

Note:
Your chosen devices interface type/number may be different than the ones shown in the map, please update the map accordingly.

Lab Work Tasks:

1. Interlink all the components.
2. Configure IP interfaces on Router, enable DHCP service. Set PC1 as DHCP clients, PC2 (Analyzer), PC3 with static IP address/subnet mask/default gateway as shown in figure 1.

   IOS Router DHCP server settings:

   ```
   ip dhcp pool pool1
   network 10.1.1.0 255.255.255.0
   default-router 10.1.1.1
   ```

3. On switch, issue *Show vlan brief* to verify if the fa0/5 and fa0/10 are in the same VLAN. If not, assign the two ports into the same VLAN (for example, VLAN1).

Lab Work Tasks:

4. Enable SPAN on SW1 so that Analyzer (PC2) can monitor Router's fa0/0 ongoing packets.

On Switch Configuration Mode, issue the following commands to set SPAN:

monitor session 1 source int g0/0 → the switch port that you want to monitor
monitor session 1 destination int g0/2 → network analyzer's port

5. Enable Telnet service on Router. (Set Username/password as **admin1**/***Cisco***)

```
Router (conf)# username admin1 password Cisco
Router (conf)# line vty 0 4
Router (conf-line)#login local
```

Review Question: how to encrypt the above password?

Router(config)#username admin1 secret Cisco

6. Capture PC1's Telnet messages to Router from Analyzer. Set a Display filter so as to figure out the telnet Username/password from the captured messages. Successful? Yes .

7. Can you find out the TCP 3-way handshake messages triggered by Telnet? Yes. If yes, fill up the Table 1.

3Way Handshake Messages

Table 1.

	1st	**2nd**	**3rd**
Source IP address	10.1.1.3	10.1.1.1	10.1.1.3
Destination IP address	10.1.1.1	10.1.1.3	10.1.1.1
TCP source port	45292	23	45292
TCP destination port	23	45292	23
TCP Sequence number	0	0	1
TCP Acknowledgment number	0	1	1
Ack bit (0 or 1)	0	1	1
Syn bit (0 or 1)	1	1	0

Analyzing Network Traffic

8. Turn Analyzer Capture session on. Now analyze DHCP messages. Issue release/renew commands on PC1 (DOS Window) to renew IP settings. Analyze DHCP PDUs, and answer the following:

   How many different types of DHCP PDUs have you observed? 2

   List here: Request and ACK

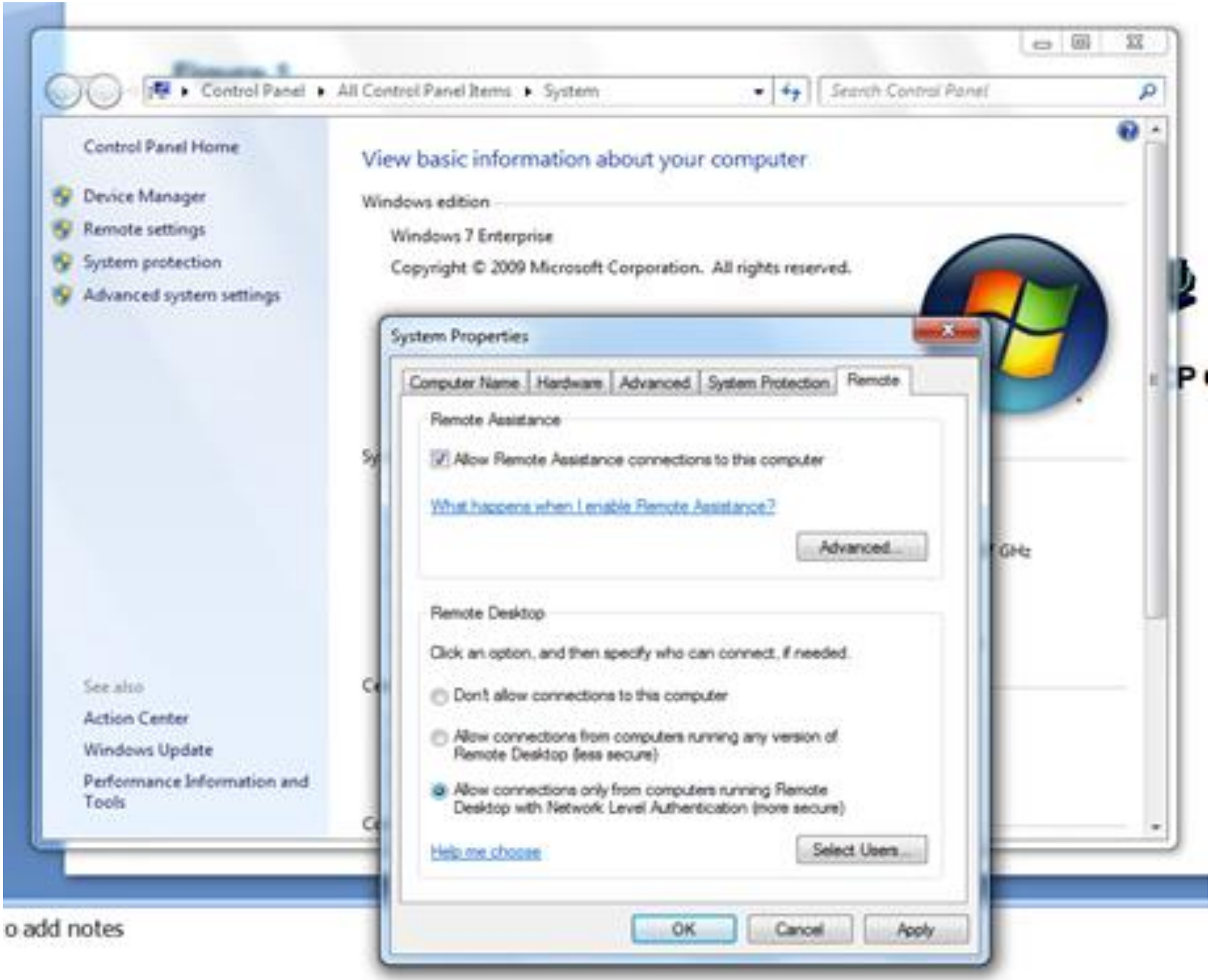
   Is DHCP UDP or TCP based? UDP

   DHCP Server end Port Number is 67

   DHCP Client end Port Number is 68

9. Capture and analyze PC1's Remote Connection to PC3 (Remote Desktop-RDP) traffic. Consult with the next page to configure RDP. How would you describe the traffic pattern in Transport Layer? (TCP or UDP, ports fixed, etc.) Payload using UDP, authentication use TLSv1.2 Server port 3389, client port dynamic.

10. Set a Access Control List on router so that Remote Connection to PC3 is allowed, the rest traffic flows are blocked.



View basic information about your computer

Windows edition

Windows 7 Enterprise

Copyright © 2009 Microsoft Corporation. All rights reserved.

System Properties

Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

Click an option, and then specify who can connect, if needed.

○ Don't allow connections to this computer

○ Allow connections from computers running any version of Remote Desktop (less secure)

● Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

Help me choose

Testing

10. Set an Access Control List on router so that Remote Connection to PC3 is allowed, the rest traffic flows are blocked.

Q1: Your ACL configuration

```
access-list 101 permit tcp any 10.2.2.0 255.255.255.0 eq 3389
access-list 101 deny ip any any
```

Q2: Apply to which interface/direction?

```
int g0/1
ip access-group 101 out
```

Q3: How does this ACL affect DHCP service?

ACL will block DHCP packet on network 10.2.2.0/24

Q4: What happens if PC1 tries to PING PC3?

The ACL will block the ICMP package

The 2nd ACL Testing

11. Enable the Router’s HTTP service. How? `ip http server`

Remove the filter of previous step from router interface. How?

```
int g0/1
no ip access-group 101 out
```

Now set a new Access Control List on router so that

- **PC1 can ping PC3,** `access-list 101 permit ICMP 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0`
- **PC1 can HTTP browse Router** `access-list 101 permit tcp 10.1.1.0 255.255.255.0 eq 80`
- **PC1 can retrieve DHCP offer from Router (DHCP Server)**

  ```
  access-list 101 permit udp 10.1.1.0 255.255.255.0 eq 67
  access-list 101 permit udp 10.1.1.0 255.255.255.0 eq 68
  ```

- **the rest traffic flows (sourced from PC1’s network) are blocked**

  ```
  access-list 101 deny ip any any
  ```

Implement, test and answer questions of the next page.

Questions

Q1: Your ACL configuration

```
access-list 101 permit ICMP 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
access-list 101 permit tcp 10.1.1.0 255.255.255.0 eq 80
access-list 101 permit udp 10.1.1.0 255.255.255.0 eq 67
access-list 101 permit udp 10.1.1.0 255.255.255.0 eq 68
access-list 101 deny ip any any
```

Q2: Apply to which interface/direction?

```
int g0/0
ip access-group 101 in
```

Q3: How does this ACL affect PC1 to PC3 Remote Desktop Connection (RDP) service?

RDP connection failed due to router blocked port 3389 of udp protocol

Q4: What happens if PC1 tries to Telnet to Router?

Connection failed due to router blocked port 23 of tcp protocol

Reflective Question

- Basic ACL creation rules:

Standard ACL filters the traffic based on source IP address. Therefore, a it must be placed on the router which is near to the destination network/host where it is denied. If we place the it near to source of the traffic, there is a chance for denial or other legitimate traffic from the source network to some other network

Note:

Lab report submission is required.