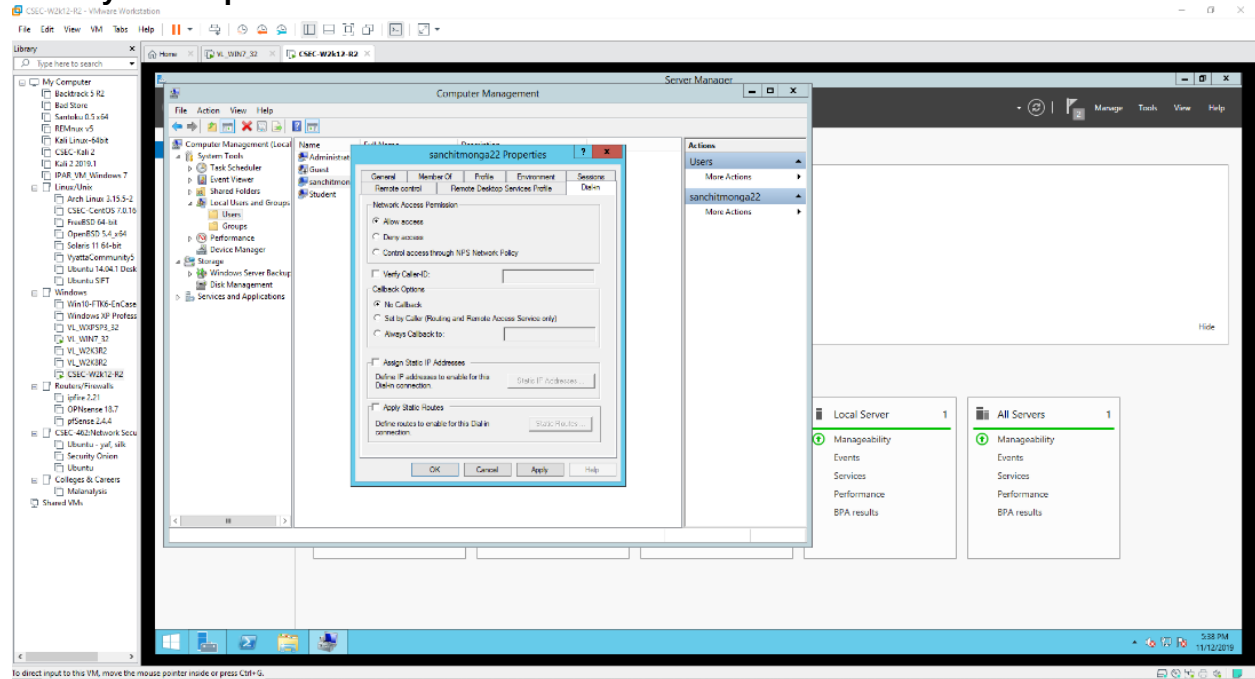


# CSEC 101 Using VPN: Lab Report

Name: Sanchit Monga

## Activity 1: Setup VPN Service and RRAS



## Activity 3: VPN Client – Network Connection Setup

### Windows 7 VM Client

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Student>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : localdomain
    IPv4 Address. . . . . : 192.168.58.128
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.58.2

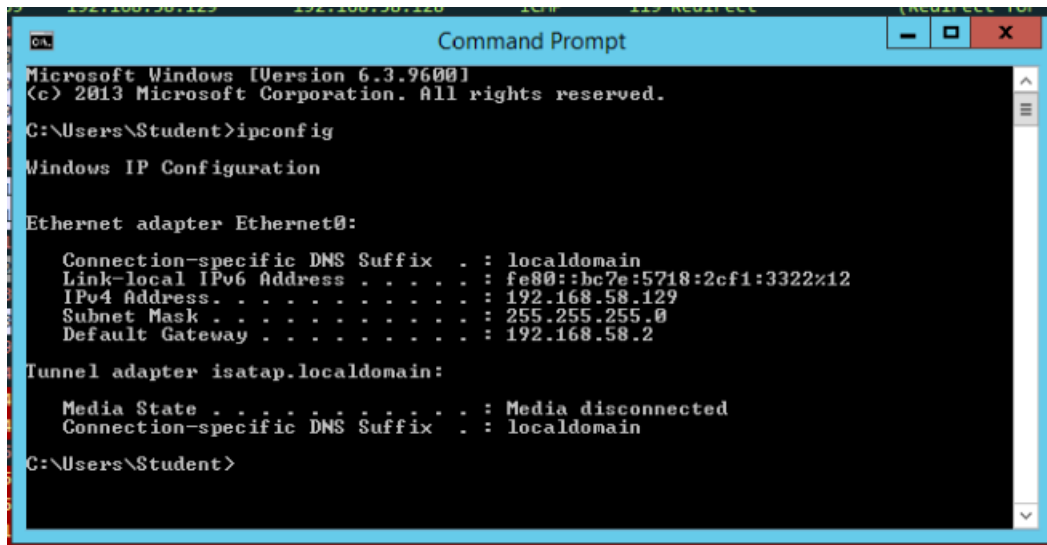
Tunnel adapter isatap.localdomain:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : localdomain

C:\Users\Student>_
```

# CSEC 101 Using VPN: Lab Report

## Windows Server 2016



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Student>ipconfig

Windows IP Configuration

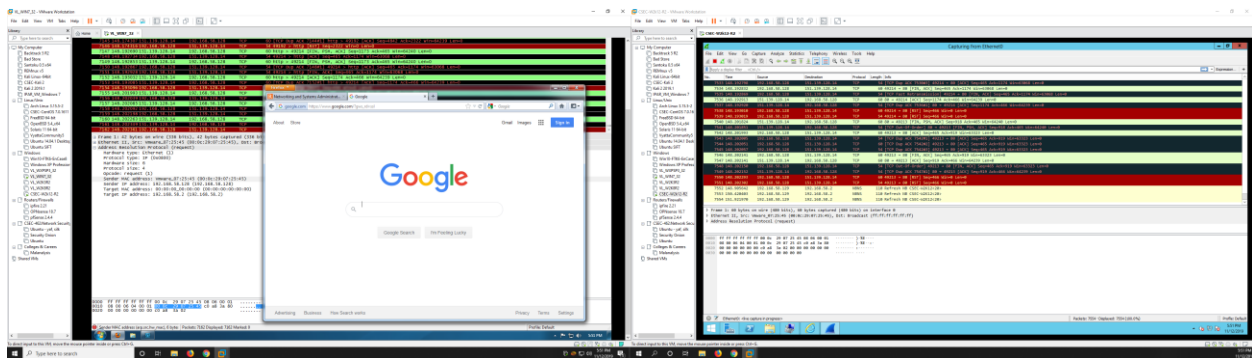
Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80:bc7e:5718:2cf1:3322%12
    IPv4 Address. . . . . : 192.168.58.129
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.58.2

Tunnel adapter isatap.localdomain:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : localdomain

C:\Users\Student>
```



1. (5 Points) After you successfully connected to the VPN server, what changes were made to the network connections.

When successfully connection to the vpn was made, the vpn basically acts as a bridge called a WAN Miniport (PPTP) which basically runs through your current local area connection.

2. (5 Points) What is the purpose of this addition?

Using MS CHAP V2 authentication and MPPE 128 encryption, it helps re-route and protect outgoing connections by sending your outgoing packets to the vpn first, then transferring it to the destination from the vpn, thus in a sense, hiding your source computer's vpn.

# CSEC 101 Using VPN: Lab Report

3. (30 Points) Fill in the following IP addresses from your setup in Activity 1 & 3.

IP Address of VPN Server Ethernet interface	192.168.58.129
IP Address of Windows 7 VM Client	192.168.58.128
IP Address Associated with the VPN client at the VPN Server: <b>You can get this IP Address after you finish Activity 3</b>	192.168.58.255

## Activity 4: Analyzing VPN traffic

### Windows 7 capture

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets. The middle pane shows the details of the selected packet (No. 1478), which is a PPP Compressed data packet. The bottom pane shows the packet bytes and the packet list.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
1478	664.114635	192.168.58.129	192.168.58.128	PPP Com	267	Compressed data
1479	664.115011	192.168.58.128	192.168.58.129	PPP Com	186	Compressed data
1480	664.115276	192.168.58.128	192.168.58.129	PPP Com	885	Compressed data
1481	664.115511	192.168.58.129	192.168.58.128	PPP Com	95	Compressed data
1482	664.115705	192.168.58.129	192.168.58.128	PPP Com	91	Compressed data
1483	664.115845	192.168.58.129	192.168.58.128	PPP Com	608	Compressed data
1484	664.154652	192.168.58.129	192.168.58.128	PPP Com	960	Compressed data
1485	664.202459	192.168.58.128	192.168.58.129	GRE	46	Encapsulated PPP
1486	664.236049	192.168.58.129	192.168.58.128	PPP Com	608	Compressed data
1487	664.236812	192.168.58.128	192.168.58.129	PPP Com	95	Compressed data
1488	664.250381	192.168.58.128	192.168.58.129	PPP Com	112	Compressed data
1489	664.251684	192.168.58.129	192.168.58.128	PPP Com	132	Compressed data
1490	664.254982	192.168.58.129	192.168.58.128	PPP Com	960	Compressed data
1491	664.255120	192.168.58.128	192.168.58.129	PPP Com	95	Compressed data
1492	664.263312	192.168.58.128	192.168.58.129	PPP Com	112	Compressed data
1493	664.264794	192.168.58.129	192.168.58.128	PPP Com	153	Compressed data
1494	664.342915	192.168.58.128	192.168.58.129	GRE	46	Encapsulated PPP
1495	668.468696	Vmware_07:25:45	Vmware_ee:10:ca	ARP	42	who has 192.168.58.129? Tell 192.168.58.128
1496	668.469139	Vmware_ee:10:ca	Vmware_07:25:45	ARP	60	192.168.58.129 is at 00:0c:29:ee:10:ca
1497	670.842821	192.168.58.128	192.168.58.129	PPTP	70	echo-Request
1498	670.843444	192.168.58.129	192.168.58.128	PPTP	74	echo-Reply
1499	671.046150	192.168.58.128	192.168.58.129	TCP	54	49201 > pptp (ack) Seq=469 Ack=333 win=65280 Len=0
1500	689.784093	192.168.58.129	255.255.255.255	DHCP	379	DHCP Request - Transaction ID 0x7elc9f0c
1501	689.787018	192.168.58.129	255.255.255.255	DHCP	379	DHCP Request - Transaction ID 0x2ac0bd0c
1502	689.789525	192.168.58.129	255.255.255.255	DHCP	379	DHCP Request - Transaction ID 0xe73314c4
1503	689.791652	192.168.58.129	255.255.255.255	DHCP	379	DHCP Request - Transaction ID 0xa5390a0a
1504	689.794243	192.168.58.129	255.255.255.255	DHCP	379	DHCP Request - Transaction ID 0xdaa4f838
1505	689.796427	192.168.58.129	255.255.255.255	DHCP	379	DHCP Request - Transaction ID 0xc28d575f
1506	689.800692	192.168.58.129	255.255.255.255	DHCP	379	DHCP Request - Transaction ID 0xff213b46
1507	689.802797	192.168.58.129	255.255.255.255	DHCP	379	DHCP Request - Transaction ID 0x417ca5c8
1508	689.805003	192.168.58.129	255.255.255.255	DHCP	379	DHCP Request - Transaction ID 0xf448b7bd
1509	689.807699	192.168.58.129	255.255.255.255	DHCP	379	DHCP Request - Transaction ID 0xc6ad3077
1510	714.874628	Vmware_07:25:45	broadcast	ARP	42	who has 192.168.58.2? Tell 192.168.58.128
1511	714.874938	Vmware_f4:75:4c	Vmware_07:25:45	ARP	60	192.168.58.2 is at 00:50:56:f4:75:4c
1512	714.874964	192.168.58.128	192.168.58.2	NBNS	110	Refresh NB WIN/32VL<20>
1513	714.875346	192.168.58.129	192.168.58.128	ICMP	138	Redirect (redirect for network)
1514	716.375012	192.168.58.128	192.168.58.2	NBNS	110	Refresh NB WIN/32VL<20>
1515	716.375009	192.168.58.129	192.168.58.128	ICMP	138	Redirect (redirect for network)
1516	717.374404	192.168.58.128	192.168.58.2	NBNS	110	Refresh NB WIN/32VL<20>
1517	717.874708	192.168.58.129	192.168.58.128	ICMP	138	Redirect (redirect for network)

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

Ethernet II, Src: Vmware\_07:25:45 (00:0c:29:07:25:45), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IP (0x0800)

Hardware size: 6

Protocol size: 4

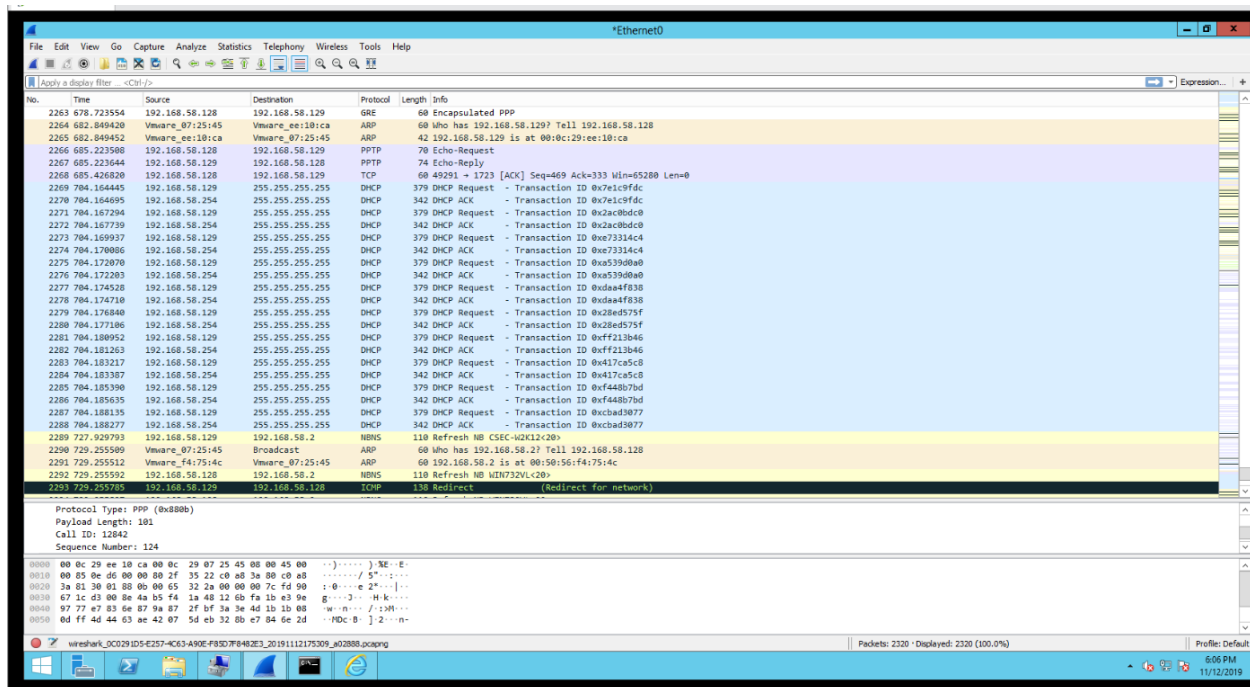
Opcode: request (1)

Sender MAC address: Vmware\_07:25:45 (00:0c:29:07:25:45)

Sender IP address: 192.168.58.128 (192.168.58.128)

# CSEC 101 Using VPN: Lab Report

## Windows Server 2016



4. (10 Points) What was different between the capture in Activity 3 and the capture in Activity 4? Use the screenshots you capture to justify your answers.  
The VPN is activated and sending all requests through the VPN server and back through encapsulated PPP packages and GRE.
5. (30 Points) What were the two protocols that Wireshark showed being used between your client and the VPN server?  
Briefly describe the function provided by this protocol  
It uses two protocols of PPTP and GRE:
  - (i) PPTP stands for point to point tunneling protocol and sends encapsulated PPP packets between the server and the client.
  - (ii) GRE stands for Generic Routing Encapsulation and creates a private point to point connection and encases multiple protocols into one for transferring data from server to client and vice versa.
6. (20 Points) What would happen if the VPN Server Firewall was on and was blocking Port number 500? What protocols use this port?

It won't be possible to establish VPN tunneling as it won't allow a vpn key to authenticate with the server.

Port 500 is used by most IPSEC-based VPN systems for the establishment of securely encrypted "tunnels" between endpoint machines.