

Tech Moment

VPN (In)security

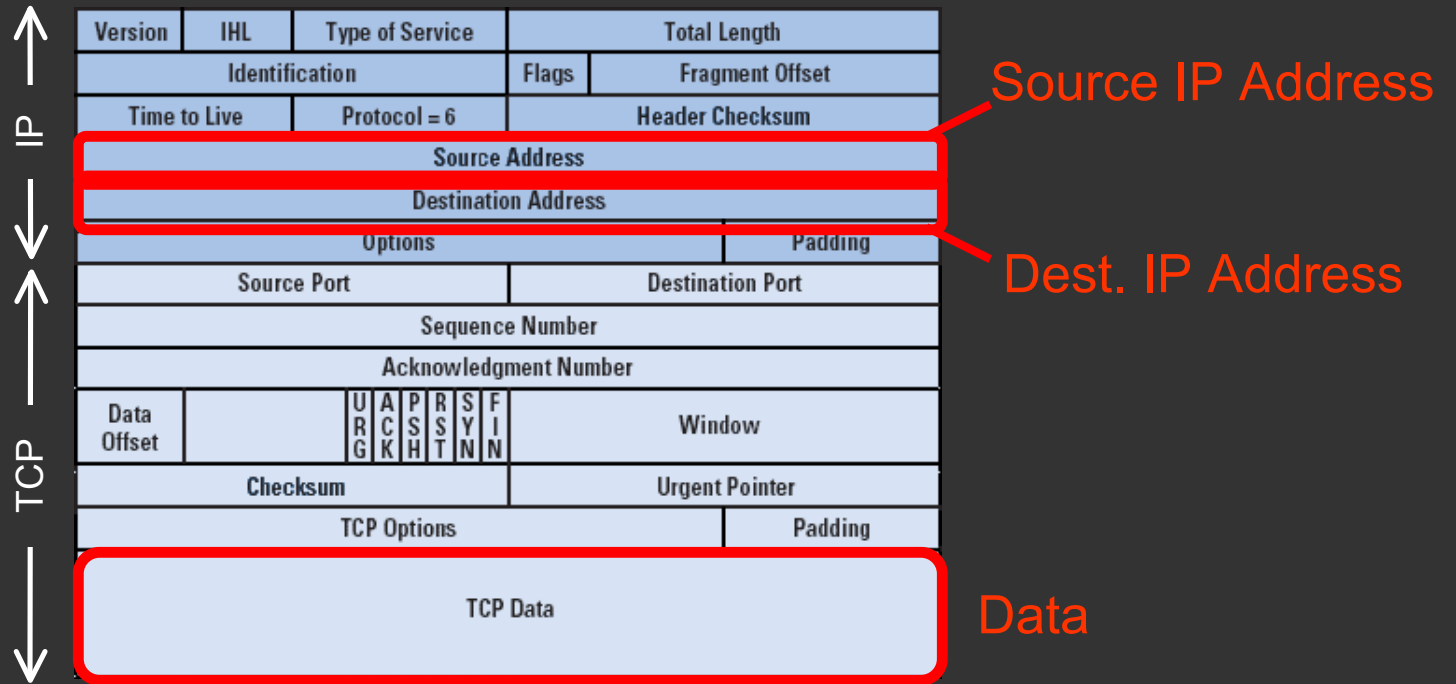
By Tom Thorpe



Packets



TCP/IP Packet Format



TCP/IP Packet Format

Version	IHL	Type of Service	Total Length																			
Identification			Flags	Fragment Offset																		
Time to Live	Protocol = 6		Header Checksum																			
Source Address																						
Destination Address																						
Options			Padding																			
Source Port		Destination Port																				
Sequence Number																						
Acknowledgment Number																						
Data Offset	<table border="1"> <tr> <td>U</td><td>A</td><td>P</td><td>R</td><td>S</td><td>F</td> </tr> <tr> <td>R</td><td>C</td><td>S</td><td>S</td><td>S</td><td>I</td> </tr> <tr> <td>G</td><td>K</td><td>H</td><td>T</td><td>N</td><td>N</td> </tr> </table>			U	A	P	R	S	F	R	C	S	S	S	I	G	K	H	T	N	N	Window
U	A	P	R	S	F																	
R	C	S	S	S	I																	
G	K	H	T	N	N																	
Checksum			Urgent Pointer																			
TCP Options			Padding																			
TCP Data																						

Ima Veteran
~~645 9062230~~
 Lomita, CA 90717



Mr. John Doe
~~216 239 3210~~
 Beverly Hills, CA
 90210

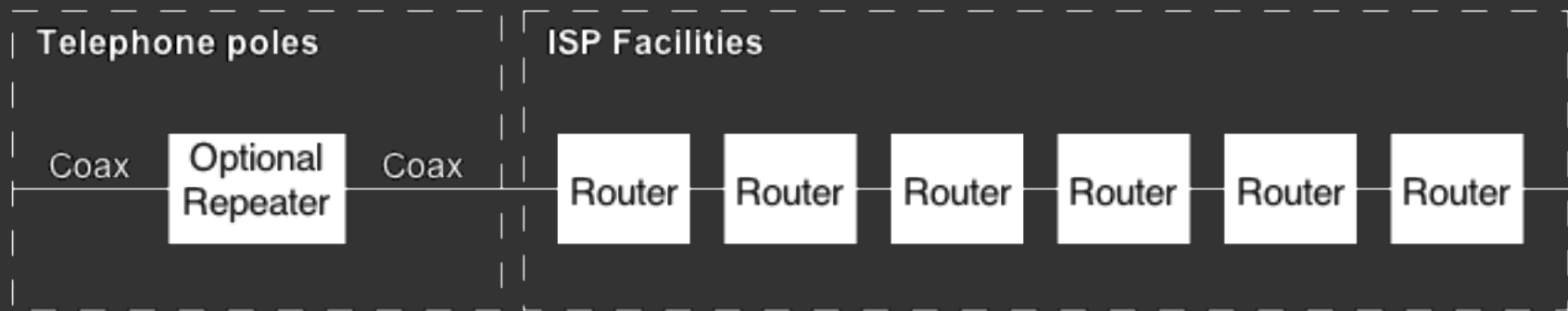
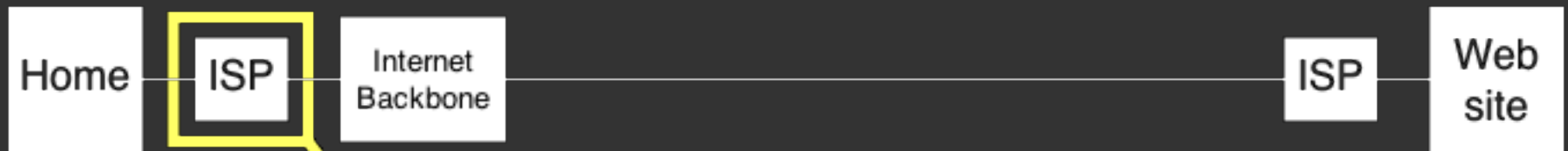


Version	IHL	Type of Service	Total Length	
Identification		Flags	Fragment Offset	
Time to Live	Protocol = 6	Header Checksum		
Source Address				
Destination Address				
Options		Padding		
Source Port	Sequence Number		Destination Port	
Acknowledgment Number				
Data Offset	U A P R S T A		Window	
Checksum		Urgent Pointer		
TCP Options			Padding	
TCP Data				

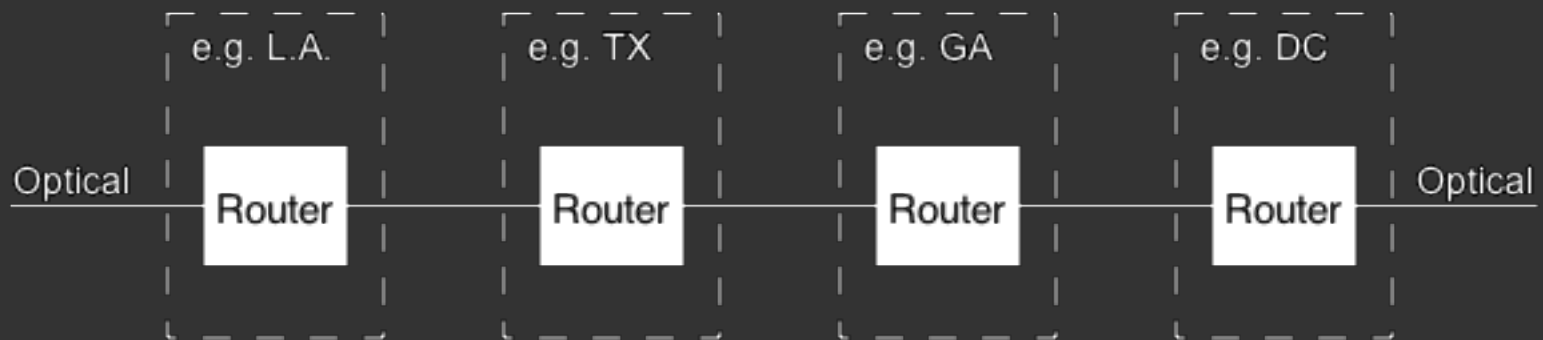


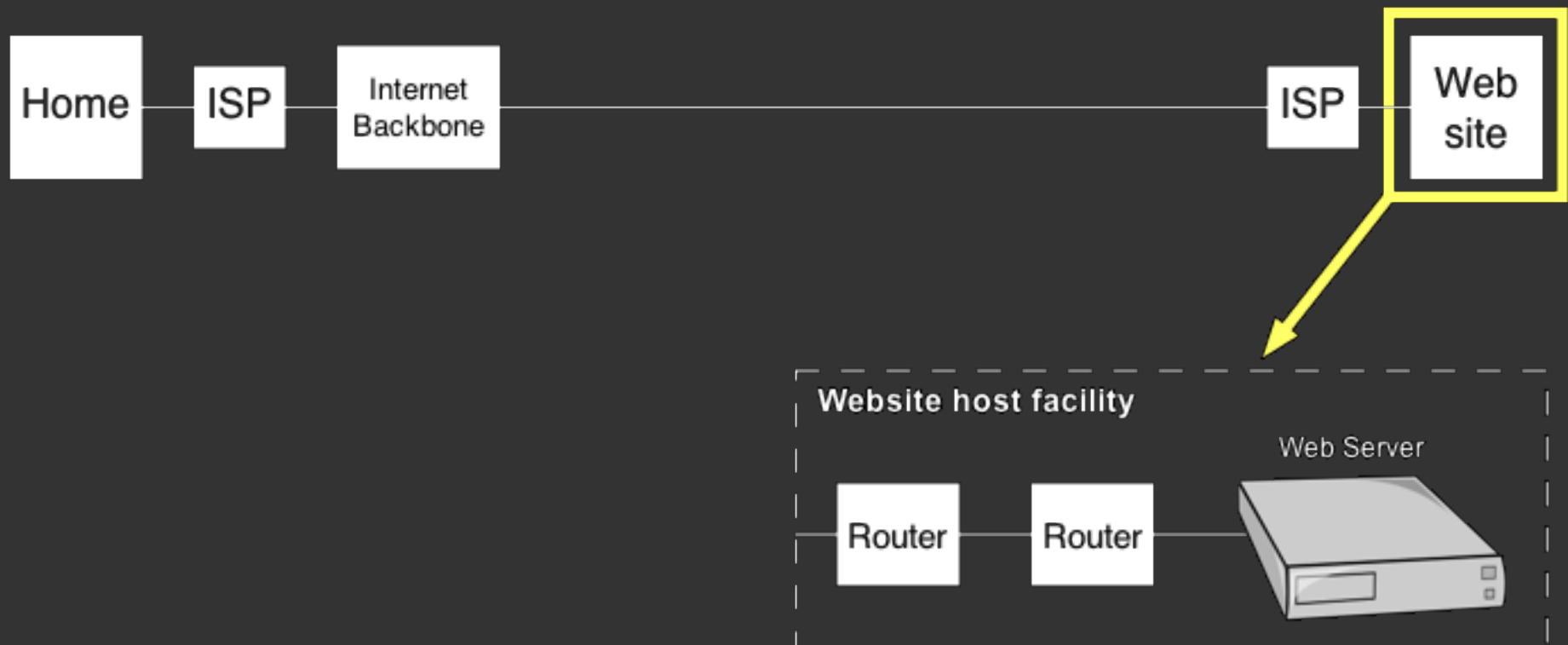
Version	IHL	Type of Service	Total Length	
Identification		Flags	Fragment Offset	
Time to Live	Protocol = 6	Header Checksum		
Source Address				
Destination Address				
Options		Padding		
Source Port	Sequence Number		Destination Port	
Acknowledgment Number				
Data Offset	U A P R S T A		Window	
Checksum		Urgent Pointer		
TCP Options			Padding	
TCP Data				





Example: sbamug.com





Example: 18 routers are involved

FCC Rules, Chapter 8 of Title 5,
“Protecting the Privacy of Customers of
Broadband and Other
Telecommunications Services”

~~Internet providers must get customers' permission before sharing their browsing history with other companies.~~

~~Internet providers must protect that data from hackers and inform customers of any breaches.~~

Killed by Congress/President in April 2017

Current Status

	<u>Collects</u>	<u>Sells</u>	<u>Targeted ads</u>
Comcast	Yes	No	Yes
AT&T	Yes	No	?
Verizon	Yes	No	Yes
Cox	No	-	-
Charter/Spectrum	Yes	No	Yes

Claimed VPN Advantages

Enhanced security

Privacy protection

Access to restricted resources

Increased speed

Adding a VPN Service

Signup and pay

Download their software

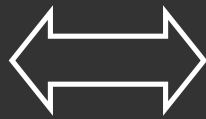
They stick themselves in the middle between you and the world

- All of your packets go to their VPN server
- It then sends them where they have to go and receives any responses
- The responses are passed back to you

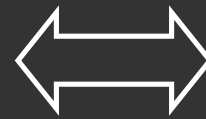


VPN Server





VPN Server



SAME TRAFFIC!

Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Live	Protocol = 6	Header Checksum	
Source Address			
Destination Address			
Options		Padding	
Source Port	Destination Port		
Sequence Number			
Acknowledgment Number			
Data Offset	U A P R S T F	Window	
Checksum		Urgent Pointer	
TCP Options		Padding	
TCP Data			

Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Live	Protocol = 6	Header Checksum	
Source Address			
Destination Address			
Options		Padding	
Source Port	Destination Port		
Sequence Number			
Acknowledgment Number			
Data Offset	U A P R S T F	Window	
Checksum		Urgent Pointer	
TCP Options		Padding	
TCP Data			



Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Live	Protocol = 6	Header Checksum	
Source Address			
Destination Address			
Options		Padding	
Source Port	Destination Port		
Sequence Number			
Acknowledgment Number			
Data Offset	U A P R S T F	Window	
Checksum		Urgent Pointer	
TCP Options		Padding	
TCP Data			

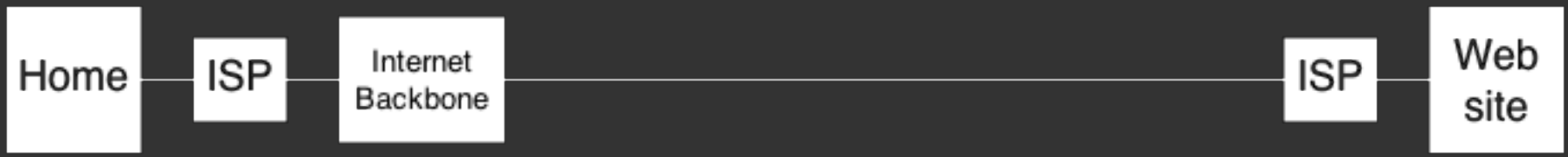
Encrypt

Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Live	Protocol = 6	Header Checksum	
Source Address			
Destination Address			
Options		Padding	
Source Port	Destination Port		
Sequence Number			
Acknowledgment Number			
Data Offset	U A P R S T F	Window	
Checksum		Urgent Pointer	
TCP Options		Padding	
TCP Data			

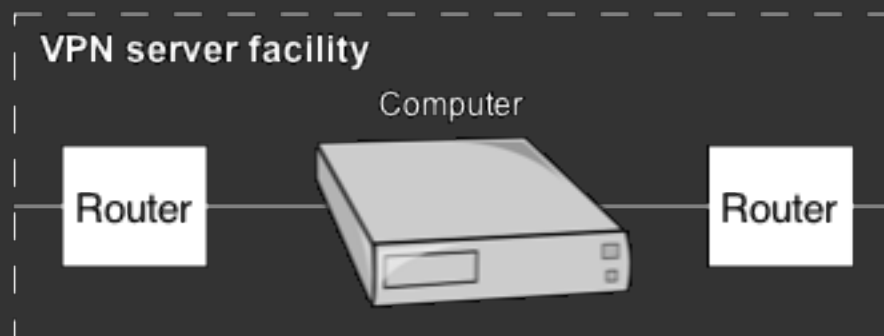
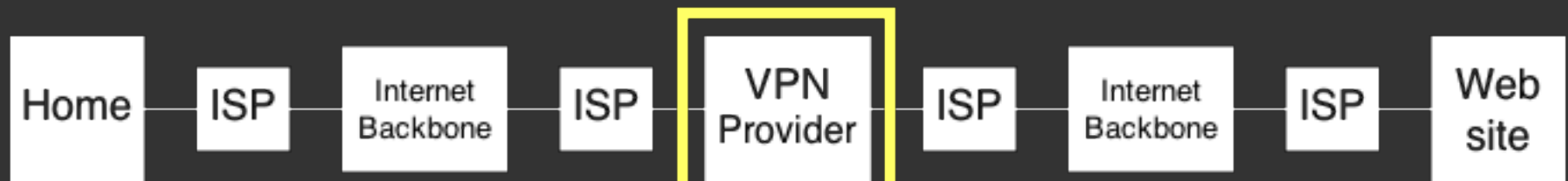


Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Live	Protocol = 6	Header Checksum	
Source Address			
Destination Address			
Options		Padding	
Source Port	Destination Port		
Sequence Number			
Acknowledgment Number			
Data Offset	U A P R S T F	Window	
Checksum		Urgent Pointer	
TCP Options		Padding	
TCP Data			

Decrypt









Traffic between you and VPN Server.
All data is encrypted.

VPN Server talks to the world.
Just like it was you.

VPN Advantages

Enhanced security

- Not really (except in a public Wi-Fi environment)
- Careful about crossing national borders

Privacy protection

- Your ISP sees you talking to just the VPN server
 - Makes for very boring tracking
- The VPN server then uses it's own IP address to talk with the world
 - Makes for interesting tracking but not back to you

Access to restricted resources

- The VPN server can be anywhere in the world
- You appear to be where the server is
- This can also hurt access (e.g. Netflix)

Increased speed

- In their wildest dreams

