My husband, an IT consultant, uses an RSA SecurID token to access his client, Citizens Bank, from our home.

HOW DOES THIS PROCESS WORK?

The RSA SecurID authentication mechanism consists of a “token,” either in the form of hardware or software, (my husband’s is hardware), which is assigned to a specific user and which generates an authentication code at set intervals based on a built-in clock and the token’s factory-encoded random key (called a “seed”). The seed is specific to each token, and is loaded into the appropriate RSA SecurID server as the tokens are purchased.

An RSA SecurID user authenticating to a network resource often needs to enter both a PIN, my husband’s was assigned to him, and the number currently displayed on their RSA SecurID token. This combination yields what is known as a two-factor authentication. It is referred to as two-factor because you must have the token AND you must know your PIN number. For further security, my husband also has to enter a valid username. The server, which also has a clock and a database of valid tokens and their associated seed records, validates a user by calculating what number the token should be showing at that precise moment in time and checking this against what the user entered.

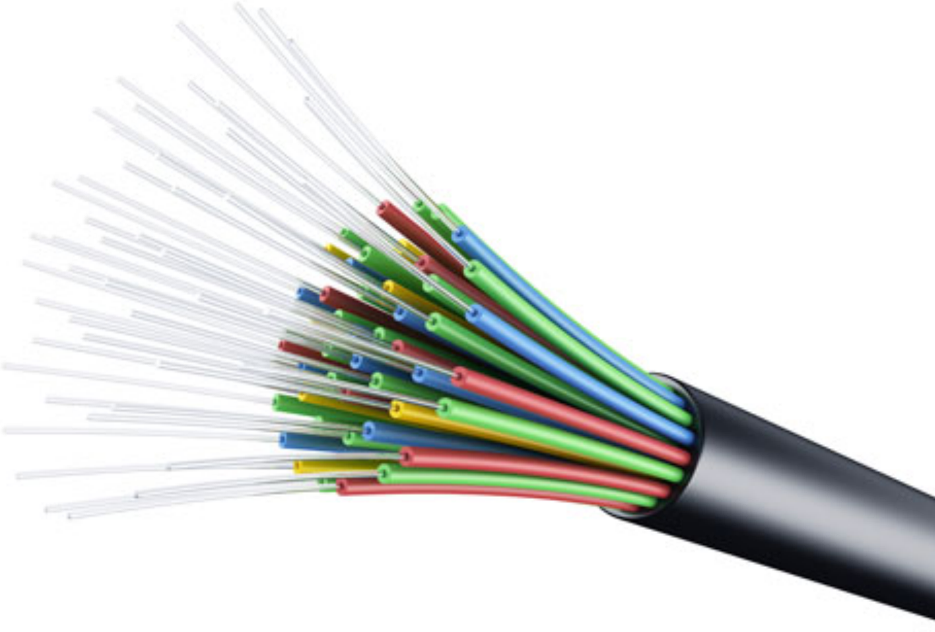
PHYSICAL LAYER

We connect WIRELESSLY

to our internet provider, Verizon FIOS.

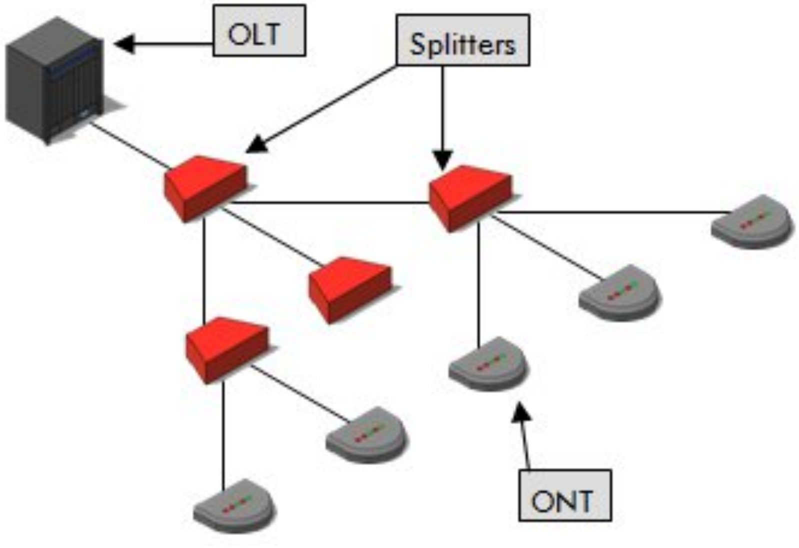
DATA LINK LAYER

Verizon FIOS Utilizes a Point-to-Multipoint Protocol



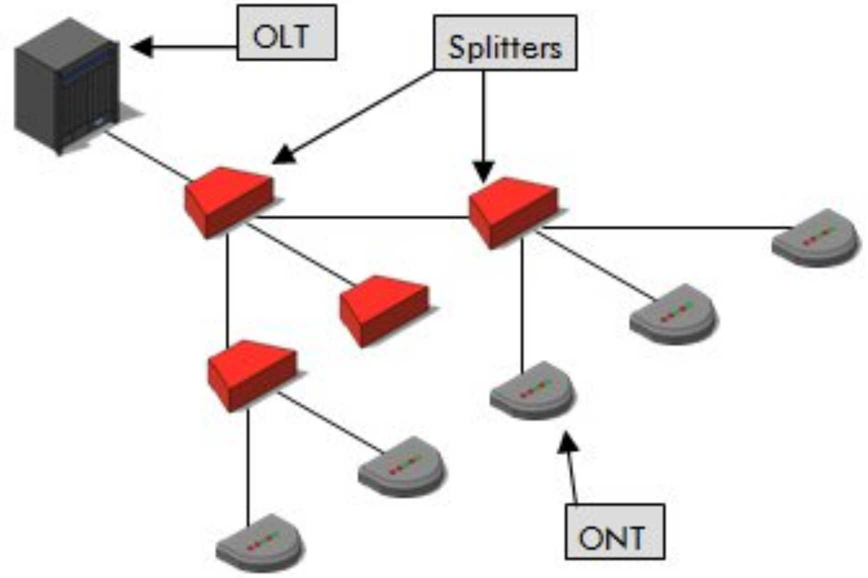
NETWORK LAYER

A single-mode fiber begins at the FIOS provider facility. After continuing out of the facility, the fiber is sent in different directions via optical splitters, enabling it to reach many subscribers (including us).



FTTP (Fiber-to-the-Premises) transmissions begin at the Verizon central switching office. OLTs (Optical Line Terminals) are pieces of equipment where these FTTP transmissions originate as they travel in and out of the Verizon network.

TRANSPORT LAYER



The fiber-based light signal reaches an optical network terminal (ONT) when it arrives at our/a subscriber's home. This ONT converts the light signal for the copper-based infrastructure that is in our home, and many others.

SESSION LAYER

My husband utilizes Internet Explorer 8 to request a session with his VPN Remote Access Login Page. Because he has accessed this page many times before, when he types this url into his address bar his laptop remembers the IP address for it and communicates to the nearest router that he wants to connect to this specific IP address. Consequently, my husband is served his requested page, where he enters his login/security information.

PRESENTATION LAYER

11011110010111010010010000110100100101

What my husband types in on the login page gets translated from application to network format so that the information can be compared to the RSA SecurID database of valid tokens with associated seed records and the numbers the tokens should be showing at that moment.

00111010010101110101010101101010111101

APPLICATION LAYER

HTTP, Hypertext Transfer Protocol, allows my husband to interact with his VPN Remote Access Login Page and, therefore, his client. In turn, HTTP allows his client to effectively communicate back to him. And in the end, our two-year-old son just loves that an RSA SecurID token makes it possible for his dad to work from home.