OSPF authentication aims to help provide a layer of security to the OSPF protocol. Many security issues can arise when not implementing OSPF authentication when using this protocol which can greatly affect an enterprise network. One of the potential issues is a rogue router coming online and injecting malicious routing information into the network. If any malicious routing information ends up being in the network, this can affect the routing table the protocols has set up. Sensitive information can be unintentionally be sent to the malicious router and end up in the wrong hands. Another potential issue that can stem from this is a Denial-of-Service attack. The malicious routing information gives the attacker access to the network, so what could happen is the attacker could intentionally cause an interruption to an enterprise network by flooding it with requests. The network then becomes overloaded with these requests and prevent tasks from being fulfilled.

Once this option is activated on each router using the OSPF protocol, the router will authenticate all routing traffic between routers by using a shared password that uniquely set with each OSPF area. There are two authentication methods mainly used by the OSPF protocol: Plain Text and MD5. Plain Text authentication is just what it sounds like, a password in plain text is added to the OSPF area which is used for OSPF routing traffic authentication. MD5 authentication uses a key and key-id. These are configured on the routers that are using them, which creates a hash value that is added to the appropriate routing traffic. The created hash value is what is used when authenticating OSPF routing traffic.