Rashan Hibbert

CST 1101

Assignment #1

IEEE 802.1X is an IEEE Standard for port-based Network Access Control. It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN. IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol over IEEE 802. 1, 2 which is known as EAPOL.3, EAPOL was originally designed for IEEE 802.3 Ethernet in 802.1X-2001, but was clarified to suit other IEEE 802 LAN technologies such as IEEE 802.11 wireless and Fiber Distributed Data Interface in 802.1X-2004.4. The EAPOL protocol was also modified for use with IEEE 802.1AE and IEEE 802.1AR (Secure Device Identity, DevID) in 802.1X-2010.5, 6 to support service identification and optional point to point encryption over the local LAN segment.

802.1X authentication involves three parties a supplicant, an authenticator, and an authentication server. The supplicant is a client device that wishes to attach to the LAN/WLAN. The term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols. The supplicant is not allowed access through the authenticator to the protected side of the network until the supplicant’s identity has been validated and authorized. The authentication procedure consists of Initialization On detection of a new supplicant; the port on the switch is enabled and set to the "unauthorized" state. In this state, only 802.1X traffic is allowed; other traffic, such as the Internet Protocol is dropped. Initiation to initiate authentication the authenticator will periodically transmit EAP-Request Identity frames to a special Layer 2 address on the local network segment. The supplicant listens on this address, and on receipt of the EAP-Request Identity frame it responds with an EAP-Response Identity frame containing an identifier for the supplicant such as a User ID. The authenticator then encapsulates this Identity response in a RADIUS Access-Request packet and forwards it on to the authentication server. The supplicant may also initiate or restart authentication by sending an EAPOL-Start frame to the authenticator, which will then reply with an EAP-Request Identity frame. Negotiation, the authentication server sends a reply to the authenticator, containing an EAP Request specifying the EAP Method. The authenticator encapsulates the EAP Request in an EAPOL frame and transmits it to the supplicant. At this point the supplicant can start using the requested EAP Method, or do an NAK ("Negative Acknowledgement") and respond with the EAP Methods it is willing to perform. Lastly authentication If the authentication server and supplicant agree on an EAP Method, EAP Requests and Responses are sent between the supplicant and the authentication server until the authentication server responds with either an EAP-Success message (encapsulated in a RADIUS Access-Accept packet), or an EAP-Failure message (encapsulated in a RADIUS Access-Reject packet). If authentication is successful, the authenticator sets the port to the authorized state and normal traffic is allowed, if it is unsuccessful the port remains in the unauthorized state. When the supplicant logs off, it sends an EAPOL-logoff message to the authenticator, the authenticator then sets the port to the unauthorized state, once again blocking all non-EAP traffic.