RSC
Ripple Software Consulting

Security +
Protocols

Author: Joseph Lee
Email: joseph@ripplesoftware.ca
Mobile: 778-725-3206

General Terms

AAA Protocols

- Provide authentication, authorization, and accounting

OSI Model Network Layers

- Layer 1 - Physical
- Layer 2 - Data Link
- Layer 3 - Network
- Layer 4 - Transport
- Layer 5 - Session
- Layer 6 - Presentation
- Layer 7 - Application

Protocol Numbers

- Can be used to specify a protocol when when configuring routers and firewalls
- ICMP = 1
- TCP = 6
- UDP = 17
- ESP = 50
- AH = 51

Tunnelling Protocols

SSL Secure Socket Layer

- **SSL v3** - RFC 6101 https://tools.ietf.org/html/rfc6101
- Primarily used to secure HTTP traffic as HTTPS
- SSL can **also encrypt other application** layer traffic such as **LDAP or SMTP**
- **Not recommend** for use anymore due to **vulnerabilities**

TLS Transport Layer Security

- **TLS v1.3** - RFC 8446 https://tools.ietf.org/html/rfc8446
- Replacement for SSL
- The command **STARTTLS** is used to upgrade a connection to encrypted

connection

IPsec Internet Protocol Security

- RFC 4301
- Provides authentication and encryption for IP traffic which is usually unencrypted in transit since public IP data is not particularly sensitive
- On the network layer of OSI model
- Uses two modes: transport and tunnel modes to protect **VPN traffic**
- Uses an **AH (authentication header - protocol ID number 51)**
- Also uses **ESP (Encapsulating security payload - protocol ID number 50)**
- **ISAKMP Internet Security Association and Key Management Protocol**
  - Used to negotiate a mutually acceptable level of authentication and encryption methods between the two hosts
  - This is called the **Security Association (SA)**
  - **ISAKMP** uses **IKE Internet Key Exchange on UDP port 500** (RFC 2408) to create security association for the VPN

Time synchronization Protocols

NTP Network Time Protocol

- Client-server protocol based on the exchange of packets of data using the UDP protocol over TCP/IP

SNTP Simple Network Time Protocol

- Adopts a much simpler approach
- Many of the complexities of the NTP algorithm are removed
- Rather than skewing time, many SNTP clients step time
- This is fine for many applications where a simple time-stamp is required
- Lacks the ability to monitor and filter multiple NTP servers
- Often a simple round-robin approach is used, where if one server fails, the next one in a list is used
- See **https://timetoolsltd.com/network-time-servers/the-difference-between-ntp-and-sntp/**

Authentication Protocol - Layer 7

PAP Password Authentication Protocol

- The oldest authentication protocol used for central logon
- Sends passwords in cleartext, so is used only as a last resort
- Used before PPP (point to point protocol)
- used with **PPP Point to Point protocol**

CHAP Challenge Handshake Authentication Protocol

- RFC-1994
- Is an **AAA protocol**

- The first **challenge-response** protocols
- The server challenges the client, and client responds
- Authentication challenges are sent from server to client periodically during the connection
- This challenges are replied to automatically by the client software
- **Passwords are not passed in cleartext**
- Authenticates to a local centralized authentication server
- Uses a **nonce hashed with the shared secret** to protect the shared secret from being exposed
- **MS-CHAP Microsoft CHAP**
  - This is the Microsoft implementation of CHAP (depreciated)
  - **Not secure:**
    - Microsoft is warning of a serious security issue in **MS-CHAP v2**, an authentication system that is mainly used in **Microsoft's Point-to-Point Tunneling Protocol (PPTP)** VPN technology
    - **MS-CHAP v2** uses a strangely convoluted combination of three DES operations
    - This combination can reliably be cracked by trying out all 2^56 possible DES keys
  - **MS-CHAP v2** can perform mutual authentication between client and server
  - Is vulnerable due to the use of the weak DES protocol
  - The key-space is only 2^56 and so vulnerable to brute-force
  - Consider L2TP, IPSec, or other secure VPN technology

IEEE 802.1x

- Part of the **IEEE 802.1** group of networking protocols
- Provides an authentication mechanism to devices wishing to attach to a **LAN** or **WLAN**
- Used for port based authentication protocol (**PNAC**)
- Can use **simple username and passwords or certificate-based PKI**
- Can be used to restrict access to VLAN or other **network resources**
- Used in many authentication protocols such as:
  - PPP, RADIUS, EAP group of protocols,
- Also used in **802.11 wireless networks** such as 802.11b,g,n
- General terms in the authentication process are:
  - Supplicant (client wishing to authenticate)
  - Authentication server (usually a RADIUS server)
  - Authenticator (in between Auth server and supplicant)
- The protocol used in 802.1X is called **EAP encapsulation over LANs** (**EAPOL**)

RADIUS Remote Authentication Dial-In User Service

- RFC 2058, 2059 (plus others), and RFC 3579 RADIUS Support for EAP
- Is an **AAA protocol**
- Centralized authentication service for **VPN** or other applications
- Can implement 802.1x (can other protocols used?)
- Can be used with **WPA2 Enterprise mode**

- Can implement **federated** logon and **SSO**
- Can be used with Microsoft domain
- **RADIUS** is compatible with **Diameter**
- **Only encrypts the password** in the authentication process
- Uses **UDP** so, RADIUS needs to include logic to detect communication problems since UDP does not correct these problems such as dropped packets, fragmented packets, corrupted packets etc.

Diameter

- Is an **AAA protocol**
- An **open-source protocol** created to overcome some limits of **RADIUS**
- **Diameter Applications** extend the base protocol to include commands such as those used in EAP
- New commands can be developed and built into the Diameter protocol
- Uses **TCP port 3868**

EAP Extensible Authentication Protocol

- Basic steps in the **EAP authentication process**
  1. The authenticator sends an **"EAP-Request/Identity"** packet to the supplicant when the client device is detected
  2. The supplicant sends an **"EAP-Response/Identity"** packet to the authenticator, which is then forwarded to the authentication (often RADIUS) server.
  3. The authentication server sends back a challenge to the authenticator, such as with a token password system
  4. The authenticator unpacks this from IP and **repackages it into EAPOL** and sends it to the supplicant.
  5. The supplicant responds to the challege via the authenticator which passes the response onto the authentication server again.
  6. If the supplicant authentication is valid, the authentication server responds with a success message.
- **EAP** provides a method for two systems to create a shared secure encryption key known as **Pairwise Master Key (PMK)**
  - **TKIP** and **CCMP (AES based)** use this key
- **LEAP Lightweight EAP**
  - Designed by CISCO
- **EAP-FAST EAP-Flexible Authentication vis Secure Tunnelling**
  - CISCO improved LEAP to include option for certificate-based authentication
- **PEAP Protected EAP**
  - Uses TLS encryption layer for extra layer of protection of data-in-transit through the network
  - Uses a certificate on the server to authenticate it to the client
  - The client does not use a certificate to authenticate to the server
- **EAP-tunnelled TLS (EAP-TTLS)**
  - Extension of PEAP to allow use of older authentication methods such as PAP (password authentication protocol)
  - Requires a certificate on the 802.1x sever but not the client

- **EAP-TLS**
    - Also an extension of PEAP
    - More secure EAP standard
    - Requires certificate on 802.1x server and all clients

TACACS+ Terminal Access Controller Access-Control System Plus

- RFC Draft https://tools.ietf.org/html/draft-ietf-opsawg-tacacs-13
- Is an **AAA Protocol**
- Not suitable for remote access over public network
- Mainly used on **LAN** for **administrator access** for management of network system and appliances
- Predecessors include:
    - **TACACS (RFC 927)** released in 1984
    - **Extended TACACS (XTACACS)**
        - Separated AAA features to different servers
- Can interact with **Kerberos** and **Microsoft Domains** using Kerberos
- Can interact with **EAP** suite of wireless protocols
- **Encrypts the entire** authentication process
- Uses multiple challenges and responses during a session
- TACACS+ uses **TCP port 49**

Kerberos

- Is an **AAA protocol**
- Network authentication mechanism for Windows Active Directory and some Unix environments known as realms
- Developed at MIT, Kerberos provides mutual authentication to prevent MITM and uses tickets to help prevent replay attacks, however some attacks exist such as **Kerberoast**
- Kerberos uses a **Key Distribution Center (KDC)** to issue **Ticket Granting Tickets (TGT)** and then tickets to network resources and services
- Tickets are used for authentication when clients access system resources
- Kerberos **V. 5** requires all systems to be **time synchronized** within **5 minutes** of each other and timestamps tickets to ensure they expire at the correct time as specified
- Kerberos uses a database of users such as **Active Directory**
- Kerberos uses symmetric key cryptography to prevent unauthorized access and ensure confidentiality
- Kerberos uses **UDP port 88**

Routing Protocols

RIP Routing Information Protocol

- Dynamic routing protocol that uses hop count as a metric to find the best path between source and destination
- Works on the application level of the OSI model

OSPF Open shortest path first

- Routing protocol used to trace all possible network paths and compare and categorize their speed

BGP Border Gateway Protocol

- Makes routing decisions based on paths, rules or network policies configured by a network administrator
- **BGP** manages how packets are routed across the internet through the exchange of routing and reachability information between nodes on the network
- Current implementations of BGP have vulnerabilities which allow an attacker to pass malicious routing information to an IPS alternating its routing pattern and causing a DoS

STP / RSTP (Rapid) Spanning Tree Protocol

- Prevents looping switch ports by plugging in a ethernet cable between two ports on the same switch
- Layer 2 protocol

Physical Protocols - Layer 1

Q.931 -
Bluetooth
PON
OTN
DSL
IEEE.802.11

- Part of the IEEE 802 set of LAN protocols
- Specifies the set of media access control (MAC) and physical layer (PHY) protocols
- Used in implementing wireless local area network (WLAN) including but not limited to 2.4 GHz, 5 GHz, and 60 GHz frequency bands
- Wireless (CSMA-CA)
- frames have fields for 4 MAC addresses (Source, Destination, Transmitter, Receiver)
- **802.11g**
- **802.11b**
- **802.11a**
- **802.11n**
- Uses multiple-output antennas (MIMO)
- MIMO increases receiver signal-capturing power by enabling antennas to combine data streams arriving from different paths and at different times
- Legacy wireless devices use Single-Input Single-Output (SISO) technology
- They can only send or receive one spatial stream at a time

IEEE.802.3
Ethernet (CSMA-CD)
Frames have fields for 2 MAC addresses
L431
TIA 449
And more.....

Data Link Layer Protocols - Layer 2

Sliding Window Protocol

- Windows size is the number of packets can fit in the window
- Sequence number are few bytes that cycle through 0,1,2,3,0,1,2,3, etc.
- Data Link layer of the OSI network model
- Data-flow is controlled through mechanisms called sliding windows
- TCP uses the different size of windows allowing for larger windows for faster data transmission and smaller windows when the connect communication connection is unreliable
- The sender can continue to send packets although it has not received a receipt confirmation until the window size is reached
- This process allows the destination to handle data from multiple sources with out resource exhaustion because the sender can adjust the transfer rate

PPP Point to Point Protocol

- RFC 1661
- First proposed by the IETF in 1989 and became a working standard in 1994
- Most widely used by Internet service providers (ISPs) to enable dial up connections
- Used with Analog, dialup, ISDN networks
- A data link layer (layer 2) communications protocol between two routers directly without any host or any other networking in between
- PPPoE Point-to-Point over Ethernet and is encapsulated in Ethernet frames
- PPPoA Point-to-Point over Asynchronous Transfer Mode is example of another older standard that uses PPP for authentication
- PPP supports three types of user authentication protocols: PAP, CHAP, and EAP

Transport Layer Protocols - Layer 4

TCP/IP

- RFC 793, RFC 1739 & RFC 2151 as well as others
- IP is Layer 2 and TCP is layer 3 protocols
- A core member of the Internet protocol suite (TCP/IP UDP)
- Can be encrypted using SSL/TLS.

UDP

- RFC 768 https://tools.ietf.org/html/rfc768
- A core member of the Internet protocol suite (TCP/IP UDP)
- Not encrypted
- UDP packets can not be greater then 512 bytes
- Does not normally support
- Used by some other protocols such as DNS, RADIUS, SNMP, RTP

ICMP Internet Control Message Protocol

- Used for testing connectivity (**ping/pathping, traceroute/tracecert**)
- Can be disabled to precent device discovery via ping

IGMP Internet Group Management Protocol

- Is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships

SNMP Simple Network Management Protocol

- Used to send error messages and other network information
- Uses **UDP port 161**, and **port 162** for errors and critical network (also called traps)
- **SNMPv3** monitors and manages network devices such as routers, switches, and printers
- Trap messages are the main form of communication between an **SNMP Agent** and an **SNMP Manager** (More: https://www.dpstele.com/snmp/trap-basics.php)

ARP Address Resolution Protocol

- **Resolves IP addresses to MAC** (media access control) hardware addresses in a data table on devices
- ARP attacks can **point NIC to false hardware addresses** to redirect or DOS network traffic

NDP Neighbour Discovery Protocol

- Performs similar function for **IPv6** that **ARP** does with **IPv4**

NAT Network Address Translation

- Is a protocol that translates *public IP address to private IP address* **and** *private address back to public*
- NAT allows intranet IP addresses from being publicly known and hence helps protect the LAN security
- **Static NAT -** Maps all private IP addresses to a single public IP address
- **Dynamic NAT -** Maps all private IP addresses to more than one public IP address and balances load between public IP addresses
- **NAT** is not **(now it is)** compatible with **IPsec**. **IPsec** can be used to create a VPN tunnel and use it with **L2TP** for encryption

PAT Port Address Translation

- Used when multiple local IPs are mapped to one public IP
- The clients port is mapped and returning communications are returned for that client, it is forwarded to the appropriate client

Session Layer Protocols - Layer 5

PPTP Point to Point Tunnelling Protocol

- Developed by Microsoft to include **VPN** capabilities in Microsoft products
- **Uses port 1723**

- Not encrypted alone

MMPE Microsoft Point-to-point encryption

- Can be used to encrypt the traffic in transit on Microsoft VPN
- Rarely used now

SAP Session Announcement Protocol

- RFC 2974
- An experimental protocol for broadcasting multicast session information
- Can use PGP to authenticate
- Authentication is optional

L2TP Layer 2 Tunnelling Protocol

- Developed jointly by Microsoft and Cisco
- A current standard for **VPN**
- A combination of **PPTP** from Microsoft and **L2F (Layer 2 Forwarding)** protocol from Cisco
- Also losing popularity to **IPSec**, and **SSL/TLS** VPNs

NetBIOS Network Basic Input Output System

- Allows an application on separate computers on the same network to communicate
- Developed in 1983

Application Protocols - Layer 7

HTTPS Secure Hypertext Transfer Protocol

- SSL/TLS handshake
  - **Client hello**
    - SYN packet
    - informs server that client wants to connect with HTTPS
    - Specifies a cipher suite the client is capable of (such as TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256)
  - **Server hello**
    - SYN ACK packets
    - The server reads the client hello and compares client preferred cipher to the server's supported ciphers
    - cipher suite from the list of su
  - **Key exchange**
    - FIN ACK packets
    - Key exchange handles exchange of keys to create symmetrically encrypted connection
    - TLS can include multiple commands in one packet
    - Change cipher specs can be requested by the client
  - **Finish**
    - FIN packet

S-HTTP Secure Hypertext Transfer Protocol

- An obsolete alternative to the HTTPS protocol for encrypting web communications carried over HTTP
- Served page data and submitted data like POST fields, leaving the initiation of the protocol unchanged
- The desired URL is not transmitted in the cleartext headers, but left blank; another set of headers is present inside the encrypted payload

Media Protocols

- **RTP Real-time transport protocol**
  - See RFC-3550 **https://tools.ietf.org/html/rfc3550**
  - Audio, video, VOIP, teleconferencing applications and devices using web-based push to talk features
  - **RTP** uses **UDP**
  - Can be used transmitted as unicast or multicast
- **RTSP - Real-time streaming protocol**
  - See RFC-2326 **http://www.rfc-editor.org/rfc/rfc2326.txt**
  - Analogous to RTP except that it can use TCP
  - Uses rtsp:// scheme in links
  - The Real Time Streaming Protocol, or RTSP, is an application-level protocol for control over the delivery of data with real-time properties
- **SRTP Secure Real-time Transport Protocol**
  - See RFC-3711 **https://tools.ietf.org/html/rfc3711**
  - Provides encryption, message authentication, and integrity for RTP
  - SRTP can also be used for unicast and multicast transmission

File Transfer Protocols

- **FTP File Transfer Protocol**
  - RFC 959
  - Insecure because it transfers data in cleartext using **TCP** on **port 21** for control signals and port 20 for data
  - FTP PASV (passive mode) uses random port for data (which can be blocked by firewall)
- **SFTP SSH File Transfer Protocol**
  - RFC Draft https://tools.ietf.org/html/draft-ietf-secsh-filexfer-13
  - SFTP uses **SSH on port 22** for the encryption tunnel
- **FTPS File Transfer Protocol over SSL**
  - Is an extension of FTP that uses TLS to encrypt traffic
  - Can be used on standard **FTP port 20** and **21**
  - **Port 989** and **990** are also used by some implementations of FTPS
- **TFTP Trivial File Transfer Protocol**
  - Uses UDP port 69
  - Has experienced many attacks
  - Commonly disabled

Remote Access Protocols

- **RADIUS**
- **Diameter**
- **TACACS**

- **SSH Secure Shell**
  - Used for remote access to device / system
  - Can be used to add encrypted layer to applications such as with SFTP
  - More secure than telnet
  - SCP can be used to copy files, SSH can be used to run remote commands on a server or with X11 applications
- **SSTP Secure Socket Tunnelling Protocol**
  - Encrypts VPN traffic using TLS on port 443
  - Alternative to IPsec
- **Network Access Protocols**
- **SMB**
- **LDAP Lightweight Directory Access Protocol**
  - The latest specification is Version 3, published as RFC 4511
  - Is an AAA protocol
  - Plays an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network
  - Basic operations of LDAP include BIND (Authenticate), ADD, DELETE, MODIFY records etc
  - Vendors have provided it as an access protocol to other services
  - Extension of **X.500** standard which contains details similar to certificates:
    - LDAP string: LDAP://CN=Name,CN=Users,DC=Domain,DC=com
      - CN=Name -> CN is short for common name
      - CN=Users -> CN is short for container
      - DC=Domain -> domain component
      - DC=com -> second domain component

DNS

- RFC 2034 & RFC 1035
- Can use either **TCP or UDP on port 53**
- Can be used to **transfer domains** or to **query a domain name for the IP address resolution** or reverse to **query a IP address for domians**