In many network deployment scenarios administrators would set-up a firewall in between various Aruba network elements. The following is a compilation of the network ports that need to be opened for proper operation of an Aruba network. Figure 1 illustrates a common deployment with the various network components. Obviously, the list does not include any user traffic that the network needs to carry.

Note: please remember that the Aruba controllers use both the loopback address and the VLAN addresses for communications with other network elements. If host specific ACLs are used, all controller IP addresses must be included.

Network Elements

Between Master controller and Local controller

1. PAPI (udp/8211 and tcp/8211)
2. IP-IP (protocol 4) - if L3 mobility is enabled

Between any two controllers

1. IP-IP (protocol 4) and PAPI (udp/8211) - if L3 mobility is enabled
2. IPSEC/NAT-T (udp/4500) - if site-to-site VPN is deployed
3. GRE (protocol 47) (if tunneling guest traffic over GRE to a DMZ controller)

Between AP and Master controller

1. PAPI (udp/8211) – If DNS is used for the AP to discover the LMS controller, an AP will first attempt to connect to the Master controller (note: allow DNS (udp/53) traffic from AP to DNS server as well).
2. PAPI (udp/8211) – All APs running as Air Monitors (AM) will have a permanent PAPI connection to the master controller.

Between AP and LMS Controller

1. FTP (tcp/20 and tcp/21)
2. TFTP (udp 69) – (for AP-52; for all other AP's, if there is no local image on the AP, e.g. a brand new AP, the AP will use TFTP to retrieve initial image)
3. NTP (udp/123)
4. SYSLOG (udp/514)
5. PAPI (udp/8211)
6. GRE (protocol 47)

Between Remote AP (IPSec) and Controller

1. NAT-T (udp/4500)
2. TFTP (UDP/69) - note: Not needed for normal operation. If the RAP looses the local image for whatever reason, TFTP is used to download the latest image.

Network Management

WebUI: Between Network Administrator's computer (Web browser) all controllers:

1. HTTP (tcp/80 and tcp/8888), or HTTPS (tcp/443 and tcp/4343)
2. SSH (tcp/22) or TELNET (tcp/23)

MMS: Between Network Administrator's computer (Web browser) and MMS Server (MM-100 Appliance or server running MMS software):

1. HTTPS (tcp/443)
2. HTTP (tcp/80) - this requirement will not be needed in future releases.
3. SSH (tcp/22) - for trouble shooting

MMS: Between MMS Server and all controllers:

1. SNMP (udp/161 and udp/162)
2. PAPI (udp/8211 and tcp/8211)

Miscellaneous

Allow traffic from the following ports on a as needed basis:

SYSLOG (udp/514) between controller and syslog servers.

TFTP (udp/69) or FTP (tcp/20 and tcp/21) between controller and software distribution server for software upgrade, or retrieving system logs.

PPTP (udp/1723) and GRE (protocol 47) to the controller if it's a PPTP VPN server

NAT-T (udp/4500) or ISAKMP (udp/500) and ESP (protocol 50) to the controller if it's an L2TP VPN server.

If a 3rd party network management system is used, allow SNMP (udp/161 and udp/162) from the NMS to all controllers (as well as AP's if Aruba OS version is prior to 2.5).

RADIUS (typically udp/1812, udp/1813, or udp/1645, udp/1646) between controller and RADIUS server.

LDAP (udp/389) or LDAPS (udp/636) between controller and LDAP server.

NTP (udp/123) between all controllers as well as MMS server to NTP server.

UDP/5555 from AP to Ethereal packet-capture station; udp/5000 from AP to Wildpackets packet-capture station.

Telnet (tcp/23) from network administrator's workstation to any AP if "telnet enable" is present in the "ap location 0.0.0" section of the controller configuration.

ICMP (protocol 1) and syslog (udp/514) between a controller and any ESI servers.

HTTP (tcp/80) or HTTPS (tcp/443) between a controller and a XML-API client.