ctrl-a	ctrl-b
(ctrl-a) #show image version --- Partition : 0:0 (/dev/usb/flash1) ****Default boot**** Software Version : ArubaOS **6.3.0.0** (Digitally Signed - Production Build) Build number : 38660 Label : 38660 Built on : Wed Jun 12 21:43:18 PDT 2013 --- Partition : 0:1 (/dev/usb/flash2) Software Version : ArubaOS 6.2.1.3 (Digitally Signed - Production Build) Build number : 39155 Label : 39155 Built on : Wed Jul 24 08:56:36 PDT 2013	(ctrl-b) #show image version --- Partition : 0:0 (/dev/usb/flash1) ****Default boot**** Software Version : ArubaOS **6.3.0.0** (Digitally Signed - Production Build) Build number : 38660 Label : 38660 Built on : Wed Jun 12 21:43:18 PDT 2013 --- Partition : 0:1 (/dev/usb/flash2) Software Version : ArubaOS 6.2.1.3 (Digitally Signed - Production Build) Build number : 39155 Label : 39155 Built on : Wed Jul 24 08:56:36 PDT 2013
(ctrl-a) #show ver Aruba Operating System Software. ArubaOS (MODEL: Aruba7210), **Version 6.3.0.0** Website: http://www.arubanetworks.com Copyright (c) 2002-2013, Aruba Networks, Inc. Compiled on 2013-06-12 at 21:43:18 PDT (build 38660) by p4build ROM: System Bootstrap, Version CPBoot 1.2.0.9 (build 35873) Built: 2012-10-24 13:51:09 Built by: p4build@re_client_35873 Switch uptime is 7 minutes 5 seconds Reboot Cause: User reboot. Supervisor Card Processor (XLP416 Rev B1 (Secure Boot) , 800 MHz) with 7382M bytes of memory. 32K bytes of non-volatile configuration memory. 7920M bytes of Supervisor Card system flash.	(ctrl-b) #show ver Aruba Operating System Software. ArubaOS (MODEL: Aruba7210), Version **6.3.0.0** Website: http://www.arubanetworks.com Copyright (c) 2002-2013, Aruba Networks, Inc. Compiled on 2013-06-12 at 21:43:18 PDT (build 38660) by p4build ROM: System Bootstrap, Version CPBoot 1.2.0.9 (build 35873) Built: 2012-10-24 13:51:09 Built by: p4build@re_client_35873 Switch uptime is 7 minutes 17 seconds Reboot Cause: User reboot. Supervisor Card Processor (XLP416 Rev B1 (Secure Boot) , 800 MHz) with 7382M bytes of memory. 32K bytes of non-volatile configuration memory. 7920M bytes of Supervisor Card system flash.
(ctrl-a) #show switch ip Switch IP Address: **172.16.0.251** Switch IP is from **Loopback** interface Switch IPv6 address is not configured.	(ctrl-b) #show switch ip Switch IP Address: **172.16.0.252** Switch IP is from **Loopback** interface Switch IPv6 address is not configured.

(ctrl-a) #show ip interface br	(ctrl-b) #show ip interface br
Interface IP Address / IP Netmask Admin Protocol vlan 1 172.16.0.253 / 255.255.255.0 up up **vlan 3 10.1.1.1 / 255.255.255.0** up up loopback 172.16.0.251 / 255.255.255.255 up up tunnel 1 unassigned / unassigned up up	Interface IP Address / IP Netmask Admin Protocol vlan 1 172.16.0.254 / 255.255.255.0 up up **vlan 2 10.1.1.2 / 255.255.255.0** up up loopback 172.16.0.252 / 255.255.255.255 up up tunnel 1 unassigned / unassigned up up
(ctrl-a) #show interface tunnel 1 Tunnel 1 is up line protocol is up Description: Tunnel Interface Source 172.16.0.251 (Loopback) Destination 172.16.0.252 Tunnel mtu is set to 1100 Tunnel is a Layer2 GRE TUNNEL Tunnel is Trusted Inter Tunnel Flooding is enabled Tunnel keepalive is enabled Tunnel keepalive interval is 10 seconds, retries 3 Heartbeats sent 8, Heartbeats lost 2 Tunnel is down 0 times **tunnel vlan 3**	(ctrl-b) #show interface tunnel 1 Tunnel 1 is up line protocol is up Description: Tunnel Interface Source 172.16.0.252 (Loopback) Destination 172.16.0.251 Tunnel mtu is set to 1100 Tunnel is a Layer2 GRE TUNNEL Tunnel is Trusted Inter Tunnel Flooding is enabled Tunnel keepalive is enabled Tunnel keepalive interval is 10 seconds, retries 3 Heartbeats sent 9, Heartbeats lost 1 Tunnel is down 0 times **tunnel vlan 2**
(ctrl-a) #packet-capture controlpath other	(ctrl-b) #packet-capture controlpath other
(ctrl-a) #ping **10.1.1.2** Press 'q' to abort. Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds: ..... **Success rate is 0 percent (0/5)**	(ctrl-b) #ping **10.1.1.1** Press 'q' to abort. Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds: ..... **Success rate is 0 percent (0/5)**
(ctrl-a) #show packet-capture controlpath-pcap 15:18:38.661628 ARP, Request who-has 10.1.1.2 tell 10.1.1.1, length 28 15:18:38.661663 ARP, Request who-has 10.1.1.2 tell 10.1.1.1, length 42 15:18:39.661475 ARP, Request who-has 10.1.1.2 tell 10.1.1.1, length 28 15:18:39.661516 ARP, Request who-has 10.1.1.2 tell 10.1.1.1, length 42 15:18:40.661463 ARP, Request who-has 10.1.1.2 tell 10.1.1.1, length 28 15:18:40.661505 ARP, Request who-has 10.1.1.2 tell 10.1.1.1, length 42	(ctrl-b) #show packet-capture controlpath-pcap 15:18:26.444040 ARP, Request who-has 10.1.1.1 tell 10.1.1.2, length 28 15:18:26.444088 ARP, Request who-has 10.1.1.1 tell 10.1.1.2, length 42 15:18:27.443904 ARP, Request who-has 10.1.1.1 tell 10.1.1.2, length 28 15:18:27.443941 ARP, Request who-has 10.1.1.1 tell 10.1.1.2, length 42 15:18:28.443890 ARP, Request who-has 10.1.1.1 tell 10.1.1.2, length 28 15:18:28.443933 ARP, Request who-has 10.1.1.1 tell 10.1.1.2, length 42

(ctrl-a) #show datapath tunnel table

Datapath Tunnel Table Entries

Flags: E - Ether encap, I - Wi-Fi encap, R - Wired tunnel, F - IP fragment OK
W - WEP, K - TKIP, A - AESCCM, G - AESGCM, M - no mcast src filtering
S - Single encrypt, U - Untagged, X - Tunneled node, 1(cert-id) - 802.1X Term-PEAP
2(cert-id) - 802.1X Term-TLS, T - Trusted, L - No looping, d - Drop Bcast/Mcast,
D - Decrypt tunnel, a - Reduce ARP packets in the air, e - EAPOL only
C - Prohibit new calls, P - Permanent, m - Convert multicast
n - Convert RAs to unicast(VLAN Pooling/L3 Mobility enabled), s - Split tunnel
V - enforce user vlan(open clients only)
H - Standby (HA-Lite)

#	Source	Destination	Prt	Type	MTU	VLAN	OVLAN	Acls	BSSID	Decaps	Encaps	Heartbeats	Flags	EncapKBytes	DecapKBytes
9	172.16.0.251	172.16.0.252	47	0	1100	0	0	0	0	0	0	00:00:00:00:00:00	16	6	13 TEFPR

(ctrl-b) #show datapath tunnel table

Datapath Tunnel Table Entries

Flags: E - Ether encap, I - Wi-Fi encap, R - Wired tunnel, F - IP fragment OK
W - WEP, K - TKIP, A - AESCCM, G - AESGCM, M - no mcast src filtering
S - Single encrypt, U - Untagged, X - Tunneled node, 1(cert-id) - 802.1X Term-PEAP
2(cert-id) - 802.1X Term-TLS, T - Trusted, L - No looping, d - Drop Bcast/Mcast,
D - Decrypt tunnel, a - Reduce ARP packets in the air, e - EAPOL only
C - Prohibit new calls, P - Permanent, m - Convert multicast
n - Convert RAs to unicast(VLAN Pooling/L3 Mobility enabled), s - Split tunnel
V - enforce user vlan(open clients only)
H - Standby (HA-Lite)

#	Source	Destination	Prt	Type	MTU	VLAN	OVLAN	Acls	BSSID	Decaps	Encaps	Heartbeats	Flags	EncapKBytes	DecapKBytes
9	172.16.0.252	172.16.0.251	47	0	1100	0	0	0	0	0	0	00:00:00:00:00:00	16	6	13 TEFPR

(ctrl-a) #show arp

Protocol	Address	Hardware Address	Interface
Internet	172.16.0.252	00:1a:1e:00:5d:e8	vlan1

(ctrl-b) #show arp

Protocol	Address	Hardware Address	Interface
Internet	172.16.0.251	00:1a:1e:00:5d:70	vlan1

(ctrl-a) #show datapath bridge table

Datapath Bridge Table Entries

Flags: P - Permanent, D - Deny, R - Roamed Client, M - Mobile, X - Xsec, A - Auth, O - Outer VLAN, T - Trusted

MAC	VLAN	Assigned VLAN	QinQ VLAN	Destination	Flags

(ctrl-b) #show datapath bridge table

Datapath Bridge Table Entries

Flags: P - Permanent, D - Deny, R - Roamed Client, M - Mobile, X - Xsec, A - Auth, O - Outer VLAN, T - Trusted

MAC	VLAN	Assigned VLAN	QinQ VLAN	Destination	Flags

00:1A:1E:00:5D:70 3 3 0 local P 00:1A:1E:00:5D:70 4095 4095 0 local P 00:20:DA:00:70:04 1 1 0 local P 00:1A:1E:00:00:00 1 1 0 local P 01:80:C2:00:00:03 1 1 0 local P 01:80:C2:00:00:00 1 1 0 local P 00:1A:1E:00:5D:E8 1 1 0 0/0/0 00:1A:1E:00:5D:70 1 1 0 local P 00:1A:1E:00:00:00 4095 4095 0 local P 00:1A:1E:00:00:00 3 3 0 local P 01:80:C2:00:00:0E 1 1 0 local P 01:80:C2:00:00:02 1 1 0 local P 00:1A:1E:00:5D:E9 1 1 0 0/0/0	00:1A:1E:00:5D:71 1 1 0 0/0/0 00:20:DA:00:70:04 1 1 0 local P 00:1A:1E:00:00:00 2 2 0 local P 00:1A:1E:00:00:00 1 1 0 local P 01:80:C2:00:00:03 1 1 0 local P 01:80:C2:00:00:00 1 1 0 local P 00:1A:1E:00:5D:E8 2 2 0 local P 00:1A:1E:00:5D:E8 1 1 0 local P 00:1A:1E:00:5D:E8 4095 4095 0 local P 00:1A:1E:00:5D:70 1 1 0 0/0/0 00:1A:1E:00:00:00 4095 4095 0 local P 01:80:C2:00:00:0E 1 1 0 local P 01:80:C2:00:00:02 1 1 0 local P
ctrl-a: delete vlan 3 and add vlan 2	
(ctrl-a) #configure t Enter Configuration commands, one per line. End with CNTL/Z (ctrl-a) (config) #interface vlan 3 (ctrl-a) (config-subif)# no ip address (ctrl-a) (config-subif)#! (ctrl-a) (config) #no interface vlan 3 (ctrl-a) (config) #! (ctrl-a) (config) #no vlan 3 (ctrl-a) (config) #! (ctrl-a) (config) #vlan 2 (ctrl-a) (config) #! (ctrl-a) (config) #interface vlan 2 (ctrl-a) (config-subif)# ip address 10.1.1.1 255.255.255.0 (ctrl-a) (config-subif)#! (ctrl-a) (config) #interface tunnel 1 (ctrl-a) (config-tunnel)# tunnel vlan 2 (ctrl-a) (config-tunnel)#	
(ctrl-a) #show ip interface br Interface IP Address / IP Netmask Admin Protocol vlan 1 172.16.0.253 / 255.255.255.0 up up	

vlan 2 **10.1.1.1 / 255.255.255.0** up up loopback 172.16.0.251 / 255.255.255.255 up up tunnel 1 unassigned / unassigned up up	
(ctrl-a) #show interface tunnel 1 Tunnel 1 is up line protocol is up Description: Tunnel Interface Source 172.16.0.251 (Loopback) Destination 172.16.0.252 Tunnel mtu is set to 1100 Tunnel is a Layer2 GRE TUNNEL Tunnel is Trusted Inter Tunnel Flooding is enabled Tunnel keepalive is enabled Tunnel keepalive interval is 10 seconds, retries 3 Heartbeats sent 43, Heartbeats lost 2 Tunnel is down 1 times **tunnel vlan 2**	
(ctrl-a) #packet-capture reset-pcap controlpath-pcap	(ctrl-b) #packet-capture reset-pcap controlpath-pcap
(ctrl-a) #ping **10.1.1.2** Press 'q' to abort. Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds: !!!!! **Success rate is 100 percent (5/5), round-trip min/avg/max = 0.165/0.5634/2.089 ms**	(ctrl-b) #ping **10.1.1.1** Press 'q' to abort. Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds: !!!!! **Success rate is 100 percent (5/5), round-trip min/avg/max = 0.174/0.2528/0.384 ms**
(ctrl-a) #show packet-capture controlpath-pcap 15:20:53.394031 ARP, Request who-has 10.1.1.2 tell 10.1.1.1, length 28 15:20:53.394079 ARP, Request who-has 10.1.1.2 tell 10.1.1.1, length 42 15:20:53.394106 ARP, Reply 10.1.1.2 is-at 00:1a:1e:00:5d:e8, length 42 15:20:53.394133 IP 10.1.1.1 > 10.1.1.2: ICMP echo request, id 3236, seq 6, length 100 15:20:53.394595 IP 10.1.1.2 > 10.1.1.1: ICMP echo reply, id 3236, seq 6, length 100 15:20:53.395137 IP 10.1.1.1 > 10.1.1.2: ICMP echo request, id 3236, seq 7, length 100 15:20:53.395258 IP 10.1.1.2 > 10.1.1.1: ICMP echo reply, id 3236, seq 7, length 100	(ctrl-b) #show packet-capture controlpath-pcap 15:20:35.584640 IP 10.1.1.1 > 10.1.1.2: ICMP echo request, id 3236, seq 6, length 100 15:20:35.584775 ARP, Request who-has 10.1.1.1 tell 10.1.1.2, length 28 15:20:35.584921 ARP, Request who-has 10.1.1.1 tell 10.1.1.2, length 42 15:20:35.584950 ARP, Reply 10.1.1.1 is-at 00:1a:1e:00:5d:70, length 42 15:20:35.584976 IP 10.1.1.2 > 10.1.1.1: ICMP echo reply, id 3236, seq 6, length 100 15:20:35.585622 IP 10.1.1.1 > 10.1.1.2: ICMP echo request, id 3236, seq 7, length 100 15:20:35.585651 IP 10.1.1.2 > 10.1.1.1: ICMP echo reply, id 3236, seq 7, length 100

15:20:53.396534 IP 10.1.1.1 > 10.1.1.2: ICMP echo request, id 3236, seq 8, length 100 15:20:53.396658 IP 10.1.1.2 > 10.1.1.1: ICMP echo reply, id 3236, seq 8, length 100 15:20:53.397913 IP 10.1.1.1 > 10.1.1.2: ICMP echo request, id 3236, seq 9, length 100 15:20:53.397986 IP 10.1.1.2 > 10.1.1.1: ICMP echo reply, id 3236, seq 9, length 100 15:20:53.399233 IP 10.1.1.1 > 10.1.1.2: ICMP echo request, id 3236, seq 10, length 100 15:20:53.399344 IP 10.1.1.2 > 10.1.1.1: ICMP echo reply, id 3236, seq 10, length 100 15:20:59.321238 IP 10.1.1.2 > 10.1.1.1: ICMP echo request, id 3236, seq 6, length 100 15:20:59.321282 IP 10.1.1.1 > 10.1.1.2: ICMP echo reply, id 3236, seq 6, length 100 15:20:59.322549 IP 10.1.1.2 > 10.1.1.1: ICMP echo request, id 3236, seq 7, length 100 15:20:59.322586 IP 10.1.1.1 > 10.1.1.2: ICMP echo reply, id 3236, seq 7, length 100 15:20:59.323900 IP 10.1.1.2 > 10.1.1.1: ICMP echo request, id 3236, seq 8, length 100 15:20:59.323929 IP 10.1.1.1 > 10.1.1.2: ICMP echo reply, id 3236, seq 8, length 100 15:20:59.325264 IP 10.1.1.2 > 10.1.1.1: ICMP echo request, id 3236, seq 9, length 100 15:20:59.325292 IP 10.1.1.1 > 10.1.1.2: ICMP echo reply, id 3236, seq 9, length 100 15:20:59.326622 IP 10.1.1.2 > 10.1.1.1: ICMP echo request, id 3236, seq 10, length 100 15:20:59.326655 IP 10.1.1.1 > 10.1.1.2: ICMP echo reply, id 3236, seq 10, length 100	15:20:35.587006 IP 10.1.1.1 > 10.1.1.2: ICMP echo request, id 3236, seq 8, length 100 15:20:35.587035 IP 10.1.1.2 > 10.1.1.1: ICMP echo reply, id 3236, seq 8, length 100 15:20:35.588347 IP 10.1.1.1 > 10.1.1.2: ICMP echo request, id 3236, seq 9, length 100 15:20:35.588376 IP 10.1.1.2 > 10.1.1.1: ICMP echo reply, id 3236, seq 9, length 100 15:20:35.589690 IP 10.1.1.1 > 10.1.1.2: ICMP echo request, id 3236, seq 10, length 100 15:20:35.589729 IP 10.1.1.2 > 10.1.1.1: ICMP echo reply, id 3236, seq 10, length 100 15:20:41.511446 IP 10.1.1.2 > 10.1.1.1: ICMP echo request, id 3236, seq 6, length 100 15:20:41.511717 IP 10.1.1.1 > 10.1.1.2: ICMP echo reply, id 3236, seq 6, length 100 15:20:41.512895 IP 10.1.1.2 > 10.1.1.1: ICMP echo request, id 3236, seq 7, length 100 15:20:41.513128 IP 10.1.1.1 > 10.1.1.2: ICMP echo reply, id 3236, seq 7, length 100 15:20:41.514236 IP 10.1.1.2 > 10.1.1.1: ICMP echo request, id 3236, seq 8, length 100 15:20:41.514345 IP 10.1.1.1 > 10.1.1.2: ICMP echo reply, id 3236, seq 8, length 100 15:20:41.515601 IP 10.1.1.2 > 10.1.1.1: ICMP echo request, id 3236, seq 9, length 100 15:20:41.515711 IP 10.1.1.1 > 10.1.1.2: ICMP echo reply, id 3236, seq 9, length 100 15:20:41.516954 IP 10.1.1.2 > 10.1.1.1: ICMP echo request, id 3236, seq 10, length 100 15:20:41.517100 IP 10.1.1.1 > 10.1.1.2: ICMP echo reply, id 3236, seq 10, length 100
(ctrl-a) # show datapath tunnel table Datapath Tunnel Table Entries ---------- Flags: E - Ether encap, I - Wi-Fi encap, R - Wired tunnel, F - IP fragment OK W - WEP, K - TKIP, A - AESCCM, G - AESGCM, M - no mcast src filtering S - Single encrypt, U - Untagged, X - Tunneled node, 1(cert-id) - 802.1X Term-PEAP 2(cert-id) - 802.1X Term-TLS, T - Trusted, L - No looping, d - Drop Bcast/Mcast,	(ctrl-b) # show datapath tunnel table Datapath Tunnel Table Entries ---------- Flags: E - Ether encap, I - Wi-Fi encap, R - Wired tunnel, F - IP fragment OK W - WEP, K - TKIP, A - AESCCM, G - AESGCM, M - no mcast src filtering S - Single encrypt, U - Untagged, X - Tunneled node, 1(cert-id) - 802.1X Term-PEAP

D - Decrypt tunnel, a - Reduce ARP packets in the air, e - EAPOL only
C - Prohibit new calls, P - Permanent, m - Convert multicast
n - Convert RAs to unicast(VLAN Pooling/L3 Mobility enabled), s - Split tunnel
V - enforce user vlan(open clients only)
H - Standby (HA-Lite)

#	Source	Destination	Prt	Type	MTU	VLAN	OVLAN	Acls	BSSID	Decaps	Encaps	Heartbeats	Flags	EncapKBytes	DecapKBytes
10	172.16.0.251	172.16.0.252	47	0	1100	0	0	0	0	0	0	00:00:00:00:00:00		16	16	4	TEFPR

2(cert-id) - 802.1X Term-TLS, T - Trusted, L - No looping, d - Drop Bcast/Mcast,
D - Decrypt tunnel, a - Reduce ARP packets in the air, e - EAPOL only
C - Prohibit new calls, P - Permanent, m - Convert multicast
n - Convert RAs to unicast(VLAN Pooling/L3 Mobility enabled), s - Split tunnel
V - enforce user vlan(open clients only)
H - Standby (HA-Lite)

#	Source	Destination	Prt	Type	MTU	VLAN	OVLAN	Acls	BSSID	Decaps	Encaps	Heartbeats	Flags	EncapKBytes	DecapKBytes
9	172.16.0.252	172.16.0.251	47	0	1100	0	0	0	0	0	0	00:00:00:00:00:00		43	18	24	TEFPR

(ctrl-a) #show arp

Protocol	Address	Hardware Address	Interface
Internet	172.16.0.252	00:1a:1e:00:5d:e8	vlan1
Internet	**10.1.1.2**	00:1a:1e:00:5d:e8	vlan2

(ctrl-b) #show arp

Protocol	Address	Hardware Address	Interface
Internet	10.1.1.1	00:1a:1e:00:5d:70	vlan2
Internet	**172.16.0.251**	00:1a:1e:00:5d:70	vlan1

(ctrl-a) #show datapath bridge table

Datapath Bridge Table Entries

Flags: P - Permanent, D - Deny, R - Roamed Client, M - Mobile, X - Xsec, A - Auth, O - Outer VLAN, T - Trusted

MAC	VLAN	Assigned VLAN	QinQ VLAN	Destination	Flags
00:1A:1E:00:5D:70	3	3	0	local	P
00:1A:1E:00:5D:70	4095	4095	0	local	P
00:20:DA:00:70:04	1	1	0	local	P
00:1A:1E:00:00:00	2	2	0	local	P
00:1A:1E:00:00:00	1	1	0	local	P
01:80:C2:00:00:03	1	1	0	local	P
01:80:C2:00:00:00	1	1	0	local	P
00:1A:1E:00:5D:E8	2	2	0	**tunnel 10**	

(ctrl-b) #show datapath bridge table

Datapath Bridge Table Entries

Flags: P - Permanent, D - Deny, R - Roamed Client, M - Mobile, X - Xsec, A - Auth, O - Outer VLAN, T - Trusted

MAC	VLAN	Assigned VLAN	QinQ VLAN	Destination	Flags
00:1A:1E:00:5D:71	1	1	0	0/0/0	
00:20:DA:00:70:04	1	1	0	local	P
00:1A:1E:00:00:00	2	2	0	local	P
00:1A:1E:00:00:00	1	1	0	local	P
01:80:C2:00:00:03	1	1	0	local	P
01:80:C2:00:00:00	1	1	0	local	P
00:1A:1E:00:5D:E8	2	2	0	local	P
00:1A:1E:00:5D:E8	1	1	0	local	P

00:1A:1E:00:5D:E8 1 1 0 0/0/0 00:1A:1E:00:5D:70 1 1 0 local P 00:1A:1E:00:5D:70 2 2 0 local P 00:1A:1E:00:00:00 4095 4095 0 local P 01:80:C2:00:00:0E 1 1 0 local P 01:80:C2:00:00:02 1 1 0 local P 00:1A:1E:00:5D:E9 1 1 0 0/0/0	00:1A:1E:00:5D:E8 4095 4095 0 local P 00:1A:1E:00:5D:70 1 1 0 0/0/0 00:1A:1E:00:5D:70 2 2 0 **tunnel 9** 00:1A:1E:00:00:00 4095 4095 0 local P 01:80:C2:00:00:0E 1 1 0 local P 01:80:C2:00:00:02 1 1 0 local P