Instructions SEC test

Introduction:

This test plan builds to encompass the most common elements and services of a MAN network. Such as data center and various customer site (small, medium, and large). The test items feed into SEC requirement to prove that it can provide a secure customer connection.

Equipment List

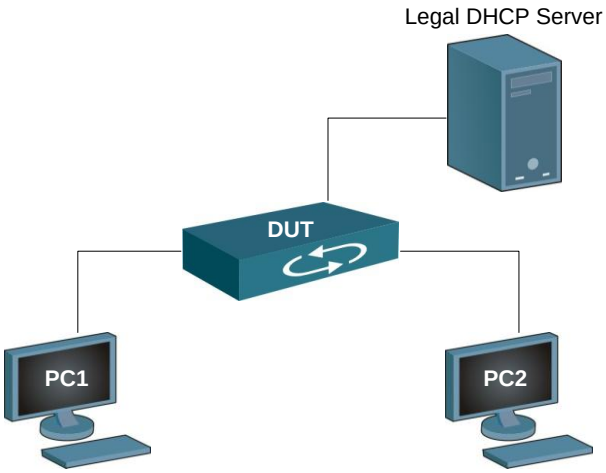
List of the proposed devices install in the topology

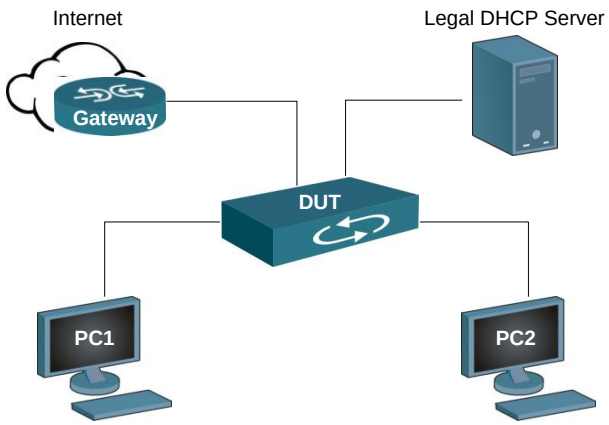
Device	Q'ty
DGS-3120	1
DGS-3200	1
DES-3528	1

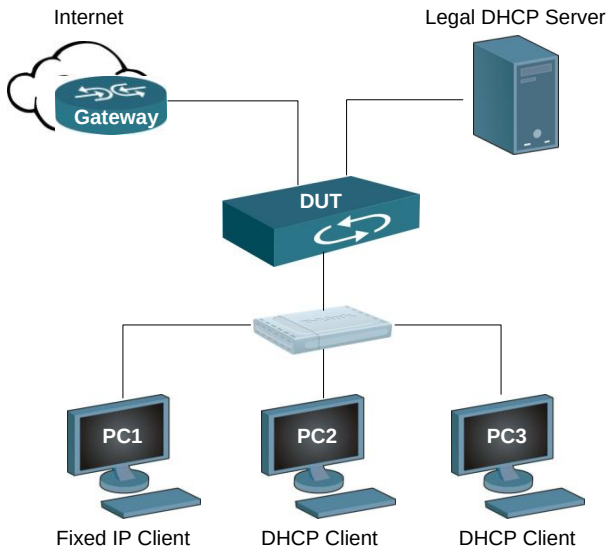
Test analyzer:

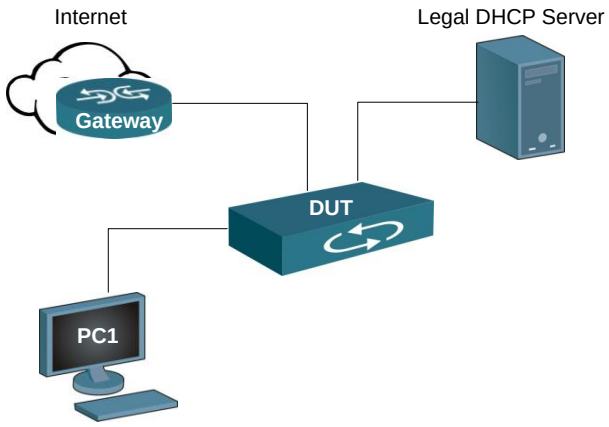
- Traffic analyzer: Smartbits or IXIA
- Traffic analyzer program: DHCPv4 server, DHCPv6 server.

Test Program:

NO.	4.1.1
Objective	So-called DHCP-snooping to filter out DHCP messages between subscribers must be located on the access ports. I.e. a subscriber must not be able to act like a DHCP-server for another subscriber.
Set-up	
Procedure	1. PC1 and PC2 uses windowsXP system 2. PC1 run DHCP service. (Unauthorized DHCP server) 3. PC2 uses DHCP client. 4. All Device resides in same VLAN. 5. Configure DHCP Server Screening to allow only Legal DHCP server to assing IP address to the client. 6. Unauthorized DHCP Server will be blocked (PC1).
Expected Results	PC2 can get IP address from legal DHCP server only.
Actual Results	PASS
Remarks	

NO.	4.1.2
Objective	It must not be possible to apply a static IP-address to get pass the port that the client is connected with, only the approved IP-address from the static entry or DHCP approved address can be used.
Set-up	
Procedure	1. PC1 and PC2 uses windowsXP system. 2. All Device resides in same VLAN. 3. All users need to use the IP address assigned by legal DHCP server. 4. Enable IMPB and apply to all users connected ports. 5. PC1 assign fixed IP address. 6. PC2 request IP address from DHCP server. 7. PC1 and PC2 ping to gateway.
Expected Results	● PC1 can NOT ping to gatewaty. ● PC2 can ping through gateway.
Actual Results	PASS
Remarks	

NO.	4.1.3
Objective	When a client is assigned one or more addresses via DHCP it must only be possible for these specific address/addresses to send traffic in through that port.
Set-up	
Procedure	1. PC1, PC2 and PC3 use windows system. 2. All devices reside in same VLAN. 3. All devices connect to DUT thru a hub. 4. All users need to use the IP address assigned by legal DHCP server. 5. Enable IMPB and apply to all users connected ports. 6. PC1 assign fixed IP address. 7. PC2 and PC3 request IP address from DHCP server. 8. ALL PCs ping to gateway.
Expected Results	● PC1 can NOT ping to gatewaty. ● PC2 and PC3 can ping through gateway.
Actual Results	PASS
Remarks	

NO.	4.1.4
Objective	If the address is not renewed via the DHCP-server a anti spoofing filter as in 4.1.2 must be applied.
Set-up	
Procedure	1. PC1 uses windowsXP system. 2. All devices reside in same VLAN. 3. Enable IMPB and apply to all users connected ports. 4. PC1 request IP address from DHCP server. 5. Block or remove DHCP server service. 6. On PC1, release IP address and renew it again. 7. PC1 can NOT get IP address from DHCP server. 8. To prevent PC1 change IP address by auto-configuration, assign it to previous IP address assigned by DHCP server.
Expected Results	PC1 can NOT ping through gateway after it loses IP address from DHCP server.
Actual Results	PASS
Remarks	

NO	4.1.5
Objective	All types of spoofing/poisoning must be prevented for the TCP/IP and ARP-protocols. I.e. the addresses which are approved from DHCP are the only addresses that must occur as the source address in TCP/IP and ARP packets.
Set-up	Same as 4.1.4
Procedure	1. PC1 uses windowsXP system. 2. All devices reside in same VLAN. 3. All users need to use the IP address assigned by legal DHCP server. 4. Enable IMPB and apply to all users connected ports. 5. PC1 assign fixed IP address. 6. PC1 send ARP traffic to Gateway. 7. PC1 send TCP traffic to Gateway. 8. PC1 send UDP traffic to Gateway. 9. PC1 send broadcast traffic to VLAN. (ARP, TCP and UDP) 10. Monitor packets receiving at gateway.
Expected Result	All traffic sending from PC1 will be dropped.
Actual Results	PASS
Remarks	

NO	4.1.6
Objective	Traceability must be added to the DHCP-requests in "L2-mode" as in option 82 for example. The access switch must not be DHCP-relay.
Set-up	Same as 4.1.4
Procedure	1 PC1 uses windowsXP system. 2 All Device resides in same VLAN. 3 Configure to add Option82 on DHCP client request packet. 4 All users need to use the IP address assigned by legal DHCP server. 5 DHCP server will assign IP address to client using DHCP option82 info. 6 PC2 request IP address from DHCP server.
Expected Result	● DHCP server can assign IP address to Client using DHCP option 82 when both server and client are in the same VLAN.
Actual Results	PASS
Remarks	

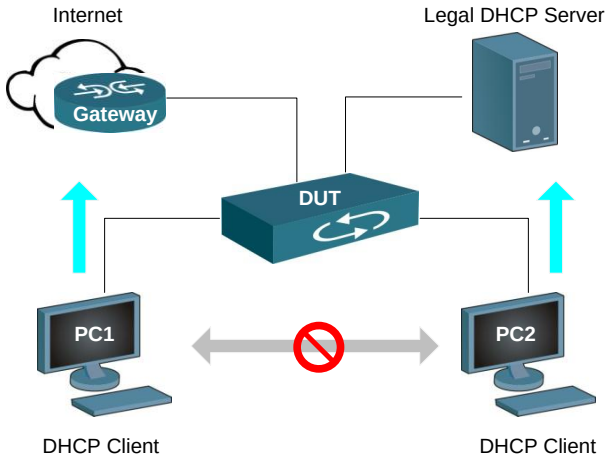
No.	4.1.7
Objective	Filter possibilities may exist between client ports. For example arbitrary TCP/UDP-ports to be filtered between subscribers.
Set-up	Same as 4.1.2
Procedure	1. PC1,PC2 use windowsXP system. 2. All devices reside in same VLAN. 3. PC1 IP Address: 192.168.1.10/24 4. PC2 IP Address: 192.168.1.11/24 5. Configure to block HTTP traffic destined to PC1 or PC2. 6. Capture packet on PC1 and PC2. 7. PC1 send HTTP packet to PC2. 8. PC2 send HTTP packet to PC2. 9. PC1 ping to PC2 in bidirectional.
Expected result	● PC1 and PC2 can ping to each other. ● PC1 should not receive HTTP packets from PC2, and vice versa.
Actual result	PASS
Remark	

No.	4.1.8
Objective	If static IP-addresses are used, the subscriber port must only allow communication for the port defined IP-address as source address in IP and ARP packets.
Set-up	Same as 4.1.4
Procedure	1. PC1 use windowsXP system. 2. All devices reside in same VLAN. 3. Enable IMPB and apply to PC1 connected ports. 4. Configure IP and MAC and port which PC1 connect to. 5. PC1 ping to gateway. 6. PC1 Change to other IP address to be different with step 4. 7. PC1 ping to gateway. 8. PC1 Change back to IP address in step 4. 9. PC1 Change to other MAC address to be different with step 4. 10. PC1 ping to gateway.
Expected result	● PC1 can ping to gateway in step 5. ● PC1 can NOT ping to gateway in step 5. ● PC1 can NOT ping to gateway in step 5.
Actual result	PASS
Remark	

No.	4.1.9
Objective	UPnP must be blocked between subscriber ports.
Set-up	Same as 4.1.2
Procedure	1. PC1 and PC2 use windowsXP system. 2. All devices reside in same VLAN. 3. On DUT, Apply filter unregister multicast group. 4. On PC1 and PC2, enable SSDP and UPnP service. 5. Monitor SSDP packets on PC1 and PC2.
Expected result	● PC1 and PC2 can NOT see SSDP packets from each other.
Actual result	PASS
Remark	

NO	4.1.10
Objective	ICMPv6 messages for RA and DHCPv6 must be blocked between subscriber ports.
Set-up	Same as 4.1.4
Procedure	1. PC1 uses windowsXP system. 2. All devices reside in same VLAN. 3. Capture packet on PC1. 4. PC1 request IPv6 address from DHCP server. 5. Internet Gateway sends IPv6 Router Advertisement (RA).
Expected Result	● PC1 should NOT receive DHCPv6 packet from DHCP server. ● PC1 should NOT receive IPv6 RA from Internet Gateway.
Actual Results	PASS
Remarks	

NO	4.1.11
Objective	There may be a possibility to filter different Ether types to only allow 0×800 and 0×806 to pass between subscriber ports. This is a good function to filter out PPPOE messages for example. In Sweden PPPOE is very unusual so that's why it isn't a must requirement.
Set-up	Same as 4.1.2
Procedure	1. All devices reside in same VLAN. 2. Configure to filter only allow IP and ARP packet on PC1 connected port. 3. Capture packet on PC2. 4. PC1 send PPPoE packets to PC2.
Expected Result	● PC1 should NOT receive any packets except IP (0x0800) and ARP (0x806) packet.
Actual Results	PASS
Remarks	

No.	4.1.12
Objective	The network may, if possible, use “force forward”/Port isolation to isolate the subscribers from each other and in that way build a more secure network. It can be managed as in 4.2 but also as a vlan / subscriber.
Set-up	
Procedure	1. PC1 and PC2 use windowsXP system. 2. All devices reside in same VLAN. 3. Enable IMPB and apply to all users connected ports. 4. Configure Traffic segmentation to filter traffic between customers. 5. PC1 and PC2 request IP address from DHCP server. 6. PC1 and PC2 ping to gateway. 7. PC1 and PC2 ping to each other.
Expected result	● PC1 and PC2 can ping to gateway. ● PC1 and PC2 can NOT ping to each other.
Actual result	PASS
Remark	