局域网攻击实例（华为）

1.ARP攻击

Feb 14 2016 08:29:42 s6700 %%01SECE/4/ARPMISS(l)[1]:Attack occurred.(**AttackType=Arp Miss Attack**, SourceInterface=XGigabitEthernet2/9/0/5, SourceIP=10.20.80.114, AttackPackets=**250 packets per second**)

Feb 14 2016 08:09:48 s6700 %%01SECE/4/ARPMISS(l)[2]:Attack occurred.(AttackType=Arp Miss Attack, SourceInterface=XGigabitEthernet2/9/0/10, SourceIP=10.20.95.80, AttackPackets=244 packets per second)

Feb 13 2016 20:46:43 s6700 %%01DEFD/4/CPCAR_DROP_LPU(l)[6]:Some packets are dropped by cpcar on the LPU in slot 8. (Protocol=icmp, Drop-Count=0389312)

Feb 13 2016 18:32:47 s6700 %%01SECE/4/ARPMISS(l)[7]:Attack occurred.(AttackType=Arp Miss Attack, SourceInterface=XGigabitEthernet1/9/0/10, SourceIP=10.20.95.82, AttackPackets=242 packets per second)

Feb 13 2016 17:56:43 s6700 %%01DEFD/4/CPCAR_DROP_LPU(l)[10]:Some packets are dropped by cpcar on the LPU in slot 8. (Protocol=icmp, Drop-Count=0906833)

Feb 13 2016 17:32:47 s6700 %%01SECE/4/ARPMISS(l)[11]:Attack occurred.(AttackType=Arp Miss Attack, SourceInterface=XGigabitEthernet1/9/0/10, SourceIP=10.20.95.82, AttackPackets=232 packets per second)

<HX-HW>dis auto-defend attack-source

Attack Source User Table (MPU):

MacAddress	InterfaceName	Vlan:Outer/Inner	TOTAL
7c1d-d96a-43cd	GigabitEthernet8/0/16	1007	400
30c7-ae95-c767	GigabitEthernet8/0/12	1005	256
1414-4b30-9bf9	GigabitEthernet12/0/23	4000	592
a0a8-cdf0-8a43	GigabitEthernet8/0/10	1004	6880
b8ee-65e4-ccae	GigabitEthernet8/0/14	1006	209680
485a-b6cd-b3e7	GigabitEthernet8/0/14	1006	56992
38bc-1ab5-2774	GigabitEthernet8/0/10	1004	320
a086-c631-3542	GigabitEthernet8/0/10	1004	432
78a8-73df-b433	GigabitEthernet8/0/16	1007	992

Total: 9

Attack Source Port Table (MPU):

InterfaceName	Vlan:Outer/Inner	TOTAL
GigabitEthernet8/0/14	1006	331952
GigabitEthernet8/0/22	1010	1088
GigabitEthernet8/0/12	1005	231008
GigabitEthernet12/0/13	43	65984
GigabitEthernet12/0/12	42	34928
GigabitEthernet12/0/23	4000	592
GigabitEthernet12/0/14	44	55616
GigabitEthernet8/0/16	1007	4496
GigabitEthernet8/0/10	1004	113488

Total: 9

Attack Source IP Table (MPU):

IPAddress	TOTAL Packets
10.13.38.74	400
172.16.0.2	448
10.13.21.200	256
10.13.30.178	56048
10.13.30.191	209536
10.13.11.255	6880
10.13.12.136	320
10.13.14.177	432
10.13.38.115	992

Total: 9

2.DHCP snooping 导致discover广播风暴

Feb 26 2014 14:06:49 S7706_1 %%01SHELL/4/LOGINFAILED(l)[0]:Failed to login. (Ip=10.10.1.87, UserName=huawei, Times=1, AccessType=TELNET)
Feb 24 2014 09:51:32 S7706_1 %%01IFPDT/4/IF_STATE(l)[1]:Interface GigabitEthernet4/0/2 has turned into UP state.
Feb 24 2014 09:51:29 S7706_1 %%01IFPDT/4/IF_STATE(l)[2]:Interface GigabitEthernet4/0/2 has turned into DOWN state.

Feb 24 2014 09:49:54 S7706_1 %%01IFPDT/4/IF_STATE(l)[3]:Interface GigabitEthernet4/0/2 has turned into UP state.
Feb 24 2014 09:49:51 S7706_1 %%01IFPDT/4/IF_STATE(l)[4]:Interface GigabitEthernet4/0/2 has turned into DOWN state.
Feb 21 2014 21:43:36 S7706_1 %%01SHELL/4/LOGINFAILED(l)[5]:Failed to login. (Ip=10.10.1.82, UserName=hauwei, Times=1, AccessType=TELNET)
Feb 17 2014 19:30:42 S7706_1 %%01SECE/3/ARPS_DROP_PACKET_SRC_MAC(l)[6]:Invalid source mac address.(SourceMAC=0000-0000-0000, SourceIP=0.0.0.0, SourceInterface=GigabitEthernet4/0/3, DropTime=2014/02/17 19:30:42)
Feb 17 2014 18:55:27 S7706_1 %%01SECE/3/ARPS_DROP_PACKET_SRC_MAC(l)[7]:Invalid source mac address.(SourceMAC=0000-0000-0000, SourceIP=0.0.0.0, SourceInterface=GigabitEthernet4/0/3, DropTime=2014/02/17 18:55:27)
Feb 17 2014 18:42:21 S7706_1 %%01SECE/3/ARPS_DROP_PACKET_SRC_MAC(l)[8]:Invalid source mac address.(SourceMAC=0000-0000-0000, SourceIP=10.10.2.2, SourceInterface=GigabitEthernet4/0/23, DropTime=2014/02/17 18:42:21)
Feb 17 2014 18:37:21 S7706_1 %%01SECE/3/ARPS_DROP_PACKET_SRC_MAC(l)[9]:Invalid source mac address.(SourceMAC=0000-0000-0000, SourceIP=0.0.0.0, SourceInterface=GigabitEthernet4/0/23, DropTime=2014/02/17 18:37:21)
Feb 17 2014 08:32:57 S7706_1 %%01SECE/4/ARPMISS(l)[10]:Attack occurred.(AttackType=Arp Miss Attack, SourceInterface=GigabitEthernet4/0/0, SourceIP=10.0.0.1, AttackPackets=39 packets per second)
Feb 11 2014 17:41:10 S7706_1 %%01SHELL/4/LOGINFAILED(l)[11]:Failed to login. (Ip=10.10.1.199, UserName=huawei, Times=1, AccessType=TELNET)
Jan 23 2014 12:50:21 S7706_1 %%01SHELL/4/LOGINFAILED(l)[12]:Failed to login. (Ip=, UserName=**, Times=1, AccessType=CON)**
Jan 19 2014 20:37:20 S7706_1 %%01SHELL/4/LOGINFAILED(l)[13]:Failed to login. (Ip=10.10.1.85, UserName=**, Times=2, AccessType=TELNET)
Jan 19 2014 20:37:16 S7706_1 %%01SHELL/4/LOGINFAILED(l)[14]:Failed to login. (Ip=10.10.1.85, UserName=huawei, Times=1, AccessType=TELNET)
Jan 17 2014 13:20:35 S7706_1 %%01SECE/4/ARPMISS(l)[15]:Attack occurred.(AttackType=Arp Miss Attack, SourceInterface=GigabitEthernet4/0/17, SourceIP=10.10.2.196, AttackPackets=94 packets per second)
Jan 17 2014 00:34:59 S7706_1 %%01SECE/4/ARPMISS(l)[16]:Attack occurred.(AttackType=Arp Miss Attack, SourceInterface=GigabitEthernet4/0/20, SourceIP=10.10.1.86, AttackPackets=63 packets per second)
Jan 16 2014 18:59:52 S7706_1 %%01SECE/4/ARPMISS(l)[17]:Attack occurred.(AttackType=Arp Miss Attack, SourceInterface=GigabitEthernet4/0/20, SourceIP=10.10.1.85, AttackPackets=82 packets per second)
Jan 16 2014 18:43:46 S7706_1 %%01SECE/4/ARPMISS(l)[18]:Attack occurred.(AttackType=Arp Miss Attack, SourceInterface=GigabitEthernet4/0/20, SourceIP=10.10.1.85, AttackPackets=84 packets per second)
Jan 16 2014 18:35:48 S7706_1 %%01SECE/4/ARPMISS(l)[19]:Attack occurred.(AttackType=Arp Miss Attack, SourceInterface=GigabitEthernet4/0/20, SourceIP=10.10.1.85, AttackPackets=79 packets per second)
Jan 12 2014 23:14:56 S7706_1 %%01CFM/4/SAVE(l)[20]:The user chose Y when deciding whether to save the configuration to the device.
Jan 12 2014 22:48:12 S7706_1 %%01CFM/4/SAVE(l)[21]:The user chose Y when deciding whether to save the configuration to the device.
Jan 12 2014 15:30:42 S7706_1 %%01SECE/4/ARPMISS(l)[22]:Attack occurred.(AttackType=Arp Miss Attack, SourceInterface=GigabitEthernet4/0/20, SourceIP=10.10.1.85, AttackPackets=79 packets per second)
Jan 12 2014 15:15:09 S7706_1 %%01SECE/4/ARPMISS(l)[23]:Attack occurred.(AttackType=Arp Miss Attack, SourceInterface=GigabitEthernet4/0/20, SourceIP=10.10.1.85, AttackPackets=79 packets per second)
Jan 12 2014 15:12:16 S7706_1 %%01CFM/4/SAVE(l)[24]:The user chose Y when deciding whether to save the configuration to the device.
Jan 12 2014 15:08:46 S7706_1 %%01SECE/4/ARPMISS(l)[25]:Attack occurred.(AttackType=Arp Miss Attack, SourceInterface=GigabitEthernet4/0/20, SourceIP=10.10.1.85, AttackPackets=79 packets per second)
Jan 12 2014 15:01:15 S7706_1 %%01CFM/4/SAVE(l)[26]:The user chose Y when deciding whether to save the configuration to the device.
Jan 12 2014 14:57:21 S7706_1 %%01CFM/4/SAVE(l)[27]:The user chose N when deciding whether to save the configuration to the device.
Jan 12 2014 14:50:14 S7706_1 %%01SECE/4/ARPMISS(l)[28]:Attack occurred.(AttackType=Arp Miss Attack, SourceInterface=GigabitEthernet4/0/20, SourceIP=10.10.1.85, AttackPackets=79 packets per second)
Jan 12 2014 14:44:33 S7706_1 %%01SECE/4/ARPMISS(l)[29]:Attack occurred.(AttackType=Arp Miss Attack, SourceInterface=GigabitEthernet4/0/20, SourceIP=10.10.1.85, AttackPackets=79 packets per second)
Jan 12 2014 14:43:25 S7706_1 %%01SNMP/4/SNMP_FAIL(l)[30]:Failed to login through SNMP. (Ip=10.10.1.85, Times=2, Reason=the community was incorrect)
Jan 12 2014 14:38:49 S7706_1 %%01SNMP/4/SNMP_FAIL(l)[31]:Failed to login through SNMP. (Ip=10.10.1.85, Times=1, Reason=the community was incorrect)
Jan 12 2014 14:13:23 S7706_1 %%01SECE/4/ARPMISS(l)[32]:Attack occurred.(AttackType=Arp Miss Attack, SourceInterface=GigabitEthernet4/0/20, SourceIP=10.10.1.85, AttackPackets=90 packets per second)
Jan 12 2014 08:36:23 S7706_1 %%01SHELL/4/LOGINFAILED(l)[33]:Failed to login. (Ip=10.10.1.82, UserName=huawei, Times=1, AccessType=TELNET)
Jan 9 2014 09:46:49 S7706_1 %%01HTTP/3/LOGINFAIL(l)[34]:User login failed. (UserName=admin, IPAddr=10.10.101.251)
Jan 9 2014 09:00:48 S7706_1 %%01HTTP/3/LOGINFAIL(l)[35]:User login failed. (UserName=administrator, IPAddr=10.10.101.248)
Jan 8 2014 20:51:12 S7706_1 %%01HTTP/4/VERIFYFAIL(l)[36]:Failed to validate HTTP verification code. (UserName=administrator, IPAddress=10.10.3.151, FailureReason=verify code not match)
Jan 8 2014 20:50:14 S7706_1 %%01HTTP/3/LOGINFAIL(l)[37]:User login failed. (UserName=admin, IPAddr=10.10.3.151)
Jan 8 2014 16:27:34 S7706_1 %%01HTTP/3/LOGINFAIL(l)[38]:User login failed. (UserName=admin, IPAddr=10.10.3.181)
Jan 8 2014 16:27:17 S7706_1 %%01HTTP/3/LOGINFAIL(l)[39]:User login failed. (UserName=guest, IPAddr=10.10.3.181)
Jan 8 2014 16:27:02 S7706_1 %%01HTTP/3/LOGINFAIL(l)[40]:User login failed. (UserName=admin, IPAddr=10.10.3.181)
Jan 8 2014 16:19:35 S7706_1 %%01SHELL/4/LOGINFAILED(l)[41]:Failed to login. (Ip=10.10.1.176, UserName=huawei, Times=1, AccessType=TELNET)
Jan 8 2014 15:10:45 S7706_1 %%01NETCONF/4/LOGOUT(l)[42]:User huawei logout from 10.10.1.18
Jan 8 2014 15:08:17 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[43]:User huawei execute command display current-configuration | include dhcp enable from 10.10.1.18 successfully.
Jan 8 2014 15:08:14 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[44]:User huawei execute command display current-configuration | include dhcp enable from 10.10.1.18 successfully.
Jan 8 2014 15:08:04 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[45]:User huawei execute command display current-configuration configuration ip-pool from 10.10.1.18 successfully.
Jan 8 2014 15:08:02 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[46]:User huawei execute command display current-configuration | include dhcp enable from 10.10.1.18 successfully.
Jan 8 2014 15:08:00 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[47]:User huawei execute command display stp brief from 10.10.1.18 successfully.
Jan 8 2014 15:08:00 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[48]:User huawei execute command display stp | include TC or TCN received from 10.10.1.18 successfully.
Jan 8 2014 15:07:57 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[49]:User huawei execute command display mac-address total-number from 10.10.1.18 successfully.
Jan 8 2014 15:07:57 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[50]:User huawei execute command display mac-address total-number from 10.10.1.18 successfully.

Jan 8 2014 15:07:57 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[51]:User huawei execute command display mac-address total-number from 10.10.1.18 successfully.
Jan 8 2014 15:07:44 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[52]:User huawei execute command display interface Ethernet0/0/0 | include Current BW from 10.10.1.18 successfully.
Jan 8 2014 15:07:44 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[53]:User huawei execute command display interface Ethernet0/0/0 | include The Maximum Frame Length is from 10.10.1.18 successfully.
Jan 8 2014 15:07:44 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[54]:User huawei execute command display interface Ethernet0/0/0 from 10.10.1.18 successfully.
Jan 8 2014 15:07:40 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[55]:User huawei execute command display version slot 4 from 10.10.1.18 successfully.
Jan 8 2014 15:07:38 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[56]:User huawei execute command display device from 10.10.1.18 successfully.
Jan 8 2014 15:07:38 S7706_1 %%01NETCONF/4/LOGIN(l)[57]:User huawei login from 10.10.1.18
Jan 8 2014 15:06:05 S7706_1 %%01CFM/4/SAVE(l)[58]:The user chose Y when deciding whether to save the configuration to the device.
Jan 8 2014 15:00:24 S7706_1 %%01CFM/4/SAVE(l)[59]:The user chose Y when deciding whether to save the configuration to the device.
Jan 7 2014 22:08:31 S7706_1 %%01NETCONF/4/LOGOUT(l)[60]:User huawei logout from 10.10.1.84
Jan 7 2014 22:07:14 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[61]:User huawei execute command display stp region-configuration from 10.10.1.84 successfully.
Jan 7 2014 22:06:41 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[62]:User huawei execute command display stp region-configuration from 10.10.1.84 successfully.
Jan 7 2014 22:06:10 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[63]:User huawei execute command display stp brief from 10.10.1.84 successfully.
Jan 7 2014 22:06:10 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[64]:User huawei execute command display stp | include TC or TCN received from 10.10.1.84 successfully.
Jan 7 2014 22:05:48 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[65]:User huawei execute command display interface Ethernet0/0/0 | include Current BW from 10.10.1.84 successfully.
Jan 7 2014 22:05:48 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[66]:User huawei execute command display interface Ethernet0/0/0 | include The Maximum Frame Length is from 10.10.1.84 successfully.
Jan 7 2014 22:05:47 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[67]:User huawei execute command display interface Ethernet0/0/0 from 10.10.1.84 successfully.
Jan 7 2014 22:05:30 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[68]:User huawei execute command display dot1x | include Quiet-times from 10.10.1.84 successfully.
Jan 7 2014 22:05:22 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[69]:User huawei execute command display dhcpv6 static user-bind all from 10.10.1.84 successfully.
Jan 7 2014 22:05:22 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[70]:User huawei execute command display dhcp static user-bind all from 10.10.1.84 successfully.
Jan 7 2014 22:05:20 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[71]:User huawei execute command display port-isolate group all from 10.10.1.84 successfully.
Jan 7 2014 22:05:20 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[72]:User huawei execute command display current-configuration | include port-isolate from 10.10.1.84 successfully.
Jan 7 2014 22:05:04 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[73]:User huawei execute command display ip routing-table statistics from 10.10.1.84 successfully.
Jan 7 2014 22:04:52 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[74]:User huawei execute command display current-configuration configuration | include traffic behavior from 10.10.1.84 successfully.
Jan 7 2014 22:04:50 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[75]:User huawei execute command display current-configuration configuration | include traffic classifier from 10.10.1.84 successfully.
Jan 7 2014 22:04:47 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[76]:User huawei execute command display current-configuration configuration | include igmp-snooping from 10.10.1.84 successfully.
Jan 7 2014 22:04:35 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[77]:User huawei execute command display current-configuration interface Vlanif4094 from 10.10.1.84 successfully.
Jan 7 2014 22:04:26 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[78]:User huawei execute command display ip pool from 10.10.1.84 successfully.
Jan 7 2014 22:04:25 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[79]:User huawei execute command display dhcp server group from 10.10.1.84 successfully.
Jan 7 2014 22:04:25 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[80]:User huawei execute command display dhcp relay all from 10.10.1.84 successfully.
Jan 7 2014 22:04:21 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[81]:User huawei execute command display ip pool from 10.10.1.84 successfully.
Jan 7 2014 22:04:04 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[82]:User huawei execute command display current-configuration configuration ip-pool from 10.10.1.84 successfully.
Jan 7 2014 22:04:02 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[83]:User huawei execute command display current-configuration | include dhcp enable from 10.10.1.84 successfully.
Jan 7 2014 22:03:49 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[84]:User huawei execute command display stp brief from 10.10.1.84 successfully.
Jan 7 2014 22:03:49 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[85]:User huawei execute command display stp | include TC or TCN received from 10.10.1.84 successfully.
Jan 7 2014 22:03:34 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[86]:User huawei execute command display mac-address total-number from 10.10.1.84 successfully.
Jan 7 2014 22:03:34 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[87]:User huawei execute command display mac-address total-number from 10.10.1.84 successfully.
Jan 7 2014 22:03:34 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[88]:User huawei execute command display mac-address total-number from 10.10.1.84 successfully.
Jan 7 2014 22:01:06 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[89]:User huawei execute command display interface Ethernet0/0/0 | include Current BW from 10.10.1.84 successfully.
Jan 7 2014 22:01:06 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[90]:User huawei execute command display interface Ethernet0/0/0 | include The Maximum Frame Length is from 10.10.1.84 successfully.
Jan 7 2014 22:01:06 S7706_1 %%01NETCONF/4/EDITCONFIG_OK(l)[91]:User huawei execute command display interface Ethernet0/0/0 from 10.10.1.84 successfully.
Jan 7 2014 22:00:57 S7706_1 %%01NETCONF/4/LOGIN(l)[92]:User huawei login from 10.10.1.84
Jan 7 2014 21:53:26 S7706_1 %%01SECE/4/ARPMISS(l)[93]:Attack occurred.(AttackType=Arp Miss Attack,

SourceInterface=GigabitEthernet4/0/20, SourceIP=10.10.1.84, AttackPackets=40 packets per second)
Jan 7 2014 21:46:07 S7706_1 %%01SECE/4/ARPMISS(l)[94]:Attack occurred.(AttackType=Arp Miss Attack, SourceInterface=GigabitEthernet4/0/20, SourceIP=10.10.1.84, AttackPackets=42 packets per second)
Jan 7 2014 21:38:27 S7706_1 %%01SECE/4/ARPMISS(l)[95]:Attack occurred.(AttackType=Arp Miss Attack, SourceInterface=GigabitEthernet4/0/20, SourceIP=10.10.1.84, AttackPackets=36 packets per second)
Jan 7 2014 21:31:34 S7706_1 %%01SECE/4/ARPMISS(l)[96]:Attack occurred.(**AttackType=Arp Miss Attack, SourceInterface=GigabitEthernet4/0/20, SourceIP=10.10.1.84, AttackPackets=68 packets per second)**
Jan 7 2014 15:56:55 S7706_1 %%01SHELL/4/LOGINFAILED(l)[97]:**Failed to login. (Ip=10.10.1.81, UserName=huawei, Times=1, AccessType=TELNET)**
Jan 7 2014 13:09:35 S7706_1 %%01SHELL/4/LOGINFAILED(l)[98]:Failed to login. (Ip=10.10.1.17, UserName=huawei, Times=1, AccessType=TELNET)