

Packet Analyst Quiz Question by Megumi Takeshita

Why you cannot connect to your office through your Nintendo

You want to play video game with your colleagues. So you connect Nintendo to office WiFi, but you never do it. So you check again RF info, channels and setting, then capture packets and filter “wlan.addr_resolved contains Nintendo” in the trace file below, why you cannot connect enterprise wireless network? Choose the adequate reason in below,

- 1: Enterprise WiFi use the different MCS(Modulation Code Set)
- 2: Nintendo’s MAC address is prohibited by office network administrator.
- 3: You use wrong Authentication mode.
- 4: You use wrong WPA1 Passphrase in 4 way handshake
- 5: You use wrong WPA2 Passphrase in 4 way handshake

The screenshot shows a Wireshark capture of network traffic. The top pane displays a list of 21 packets. Packet 21 is selected, and the bottom pane shows its details:

- Frame 21: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
- Radiotap Header v0, Length 20
- 802.11 radio information
 - IEEE 802.11 Association Response, Flags:C
 - Type/Subtype: Association Response (0x0001)
 - Frame Control Field: 0x1000
 - .000 0001 0011 1010 = Duration: 314 microseconds
 - Receiver address: Nintendo_35:63:78 (9c:e6:35:35:63:78)
 - Destination address: Nintendo_35:63:78 (9c:e6:35:35:63:78)
 - Transmitter address: Cisco_11:11:11 (00:00:0c:11:11:11)
 - Source address: Cisco_11:11:11 (00:00:0c:11:11:11)
 - BSS Id: Cisco_11:11:11 (00:00:0c:11:11:11)
 - 0000 = Fragment number: 0
 - 0000 0000 0001 = Sequence number: 1
 - Frame check sequence: 0x465da2df [correct]
 - [FCS Status: Good]
 - IEEE 802.11 wireless LAN
 - Fixed parameters (6 bytes)
 - Capabilities Information: 0x0031
 - Status code: Invalid AKMP (0x002b)
 - ..00 1000 0011 0000 = Association ID: 0x0030
 - Tagged parameters (32 bytes)
 - Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
 - Tag: Vendor Specific: Microsoft Corp.: WPA/WWE: Parameter Element

The bottom status bar shows: IEEE 802.11 wireless LAN (wlan). 24 / 1000 | パケット数: 21 | 表示: 21 (100.0%) | プロファイル: Default

Answer 3: You use wrong Authentication mode.

Explanation

The good way to troubleshoot wireless network problems, check which point packets are stacked and look deeply in the trace file.

1: Enterprise WiFi use the different MCS (Modulation Code Set)

You never see Association frames if STA and AP use the different MCS,

2: Nintendo's MAC address is prohibited by office network administrator.

MAC filtering settings are not used in this trace because there are no such status code.

3: You use wrong Authentication mode.

Correct, please check each Association Response in the trace file and look deeply in the last #21 packet, you may find the Status code field in Fixed parameters of IEEE 802.11 wireless LAN header. It shows "Invalid AKMP" which means Authentication and Key Management Protocol (AKMP) is invalid. So the mismatch of authentication methods such as Pre-Shared-Key and IEEE802.1x is the problem.

4,5: You use wrong WPA Passphrase in 4 way handshake

If WPA passphrase is wrong, you may see many EAPOL 4way handshake packets (message 1 and 2) in the trace file.