Bekannte Portsecurity-Probleme - (Portsecurity wurde durch 802.1X-Athentifizierung abgelöst)

PortSecurity Violation (allgemeine Hinweise)

Soll-MAC-Adresse	vom AV gemeldete und am Anschluss eingestellte MAC-Adresse
Ist-MAC-Adresse	letzte MAC-Adresse, die am betreffendem Anschluss aktiv war (unmittelbar vor der Abschaltung)

Mögliche Ursachen

Zum Zeitpunkt der Mailgenerierung sind die Anschlussdaten bereits gelöscht (z.B. bei -shutdown- an einem NOMADEN-Anschluss)

Soll-MAC-Adresse: 000000000000

Es kann genau dann zu Problemen kommen wenn an diesen NOMADEN-Anschlüssen mobile Stationen betrieben werden, die noch an einem FEST-Anschluss (bisher auch als HEIMAT-Anschluss bezeichnet) gemeldet sind.

Workaround

Diesen "Heimat-Anschluss" auch als NOMADEN-Anschluss anmelden

Aktive DECNET-Umgebung/ DECNET-Treiber:

Ist-MAC-Adresse: beginnt mit AA z.B. AA000400990D

Bitte DECNET deinstallieren oder wenn unbedingt benötigt die DECNET- MAC zusätzlich nachmelden

Fehlerhafte Netzkarten / Netzkartentreibersoftware (meist nur unter hoher Last)

Bekannte Beispiele

3Com	Ist-MAC-Adresse: Ziffer 2 statt 0 an 2.Stelle z.B. 02104B4D8AFE (statt richtig: 00104B4D8AFE)
APPLE	Ist-MAC-Adresse: 4 Ziffern werden vorangestellt, Rest abgeschnitten z.B. 38DB00A04024 (statt richtig: 00A040244FE1)
BELL	Ist-MAC-Adresse: 4 Ziffern (1440 o. FFFF) werden vorangestellt, Rest abgeschnitten z.B. 144000001C01 (statt richtig: 00001C014BFF)
BILLIONTON	Ist-MAC-Adresse: Ziffer 2 statt 0 an 2.Stelle .2..... (siehe 3Com) z.B. 0210603B07DC (statt richtig: 0010603B07DC)
DAYNA	Ist-MAC-Adresse: 4 Ziffern (0000) werden nachgestellt, vordere Teil abgeschnitten z.B. 191F67E50000 (statt richtig: 0080191F67E5)
EDIMAX	Ist-MAC-Adresse: 4 Ziffern (1440) werden vorangestellt, Rest abgeschnitten z.B. 144000001C01 (statt richtig: 00001C014BFF) (siehe BELL)
HP	Ist-MAC-Adresse: 2 Ziffern (08) werden nachgestellt, vordere Teil abgeschnitten z.B. 01E633B7E908 (statt richtig: 0001E633B7E9) betrifft zumindest HP JetDirect (HP-Call 1330305081)
SMC	Ist-MAC-Adresse: beginnt mit IP-Adresse (hexadezimal) 8D23..... (= 141.35.x.x) z.B. 8D231AA58D23 (statt richtig: 00E029744D42)

VMware-Installationen

Ist-MAC-Adresse: beginnt mit 005056.....
muss meist nach jeder Installation zusätzlich angemeldet werden bzw kann für jede VMware-Instanz fest vorgegeben werden mittels eines Eintrages im Konfigurationsfile: ethernet0.address = "MAC Adresse" (z.B.: "00:56:56:00:F4:40") Diese VMware-Instanzen dürfen dann natürlich nicht zur gleichen Zeit laufen. Wenn mehrere virtuelle Netzkarten konfiguriert werden, dann sollten die MAC-Adressen für ethernet1.address und weitere in den VMware-Instanzen auch gleich sein (aber verschieden von ethernet0.address).

Doppelte IP-Adressen

Im Zusammenhang mit der Erkennung doppelter IP-Adressen senden Windows-Systeme gratious ARP-Pakete (gARP). Dabei handelt es sich um ARP-Response-Pakete die unaufgefordert gesendet werden, also ohne vorherigen ARP-Request. Stellt Windows einen Adresskonflikt zur eigenen IP-Adresse fest, wird versucht allen Teilnehmern am Netz mittels Senden eines gratious ARP-Response wieder die ursprüngliche MAC-Adresse zu dieser IP-Adresse mitzuteilen. Da dies aber nicht die eigene MAC-Adresse ist muss folglich die PortSecurity zuschlagen und unterbindet somit auch Dup-IP-Address Konflikte. Dabei wird also immer der Anschluss deaktiviert an dem der Dup-IP-Address Konflikt auftrat – oder andersherum: Wer eine IP-Adresse zuerst hat behält diese. Praktisch bedeutet das: Ist man sich sicher, dass am betreffenden Anschluss kein anderes Gerät aktiv war, ist es sinnvoll im Netz nach dem Standort der „Ist-MAC-Adresse“ zu suchen um den Konfliktteilnehmer zu finden.

Weitere mögliche Ursachen

- Vertauschung von Anschlusskabeln
- Vertauschung von Endgeräten
- Sicherheitsverstöße: z.B. illegaler Anschluss von Endsystemen bzw. gezielte Adressmanipulation u.U. zum Abhören des Datenverkehrs mittels Übernahme- / Relaying-Tool