Whitepaper: IP-MAC-Port-Binding (IMPB)

In Unternehmen spielt heute die Verfügbarkeit der IT-Infrastruktur, wie z.B. Telefonie und Netzwerk, eine sehr große Rolle. Ohne diese Infrastruktur gehen Anrufe und auch Aufträge verloren, können Projekte nicht bearbeitet und Kunden nicht erreicht werden.

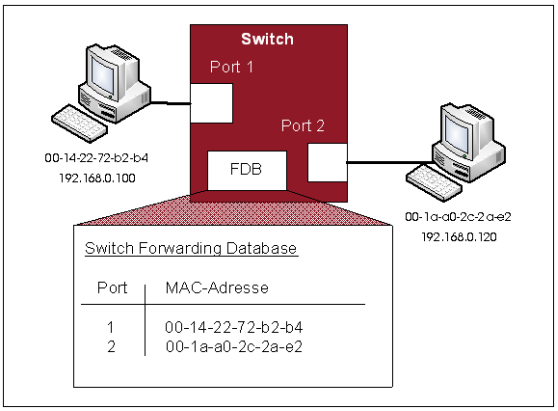
Der Ausfall eines Netzwerkes oder eines Netzwerksegmentes kann ungewollt, z.B. im Rahmen einer Fehlkonfiguration oder eines defektes Gerätes, passieren. Aber auch eine gewollte Beeinflussung oder bewusste Angriffe können zu einem Stillstand des Netzes führen. Zusätzlich ist durch entsprechende Angriffe ein Ausspähen oder Manipulieren sensibler Daten möglich, wie z.B. durch eine Man-in-the-Middle Attacke.

Demzufolge müssen in einem Netzwerk Maßnahmen ergriffen werden, die die Wahrscheinlichkeit eines Ausfalls minimieren. Hierfür wurde, für die D-Link xStack Familie das Feature „IP-MAC-Port-Binding" (IMPB) entwickelt, welches das Netzwerk vor ungewollten und nicht autorisierten Eingriffen in die Konfiguration schützen und Ausfälle sowie Angriffe wirksam verhindern kann.

Adressierung im Netzwerk

Die Kommunikation in einem geswitchten Layer 2 Netzwerk verläuft nach folgendem Schema:

- **Ein Sender**, z.B. ein PC, möchte an einen Empfänger, z.B. einen Server, ein Datenpaket senden. Er hat dafür eine IP-Adresse als Zieladresse. Um an die Empfänger MAC-Adresse zu gelangen sendet der Sender einen sogenannten ARP-Broadcast aus (ARP → Address Resolution Protocol). In diesem Paket stehen sowohl die IP- und MAC-Adresse des Senders als auch die IP-Adresse des Empfängers.
- **Der Switch** empfängt den ARP-Broadcast auf dem Port, an welchem der Sender angeschlossen ist, übernimmt die MAC-Adresse des Senders in seine Forwarding Database (FDB) und sendet den Request an allen aktiven Ports raus. Somit erreicht dieses Paket auch den gewünschten Empfänger.
- **Der Empfänger** antwortet mit einem ARP-Reply direkt an den Sender, in welchem seine eigene MAC-Adresse vermerkt ist. Auf dem Switch, an welchem der Empfänger angeschlossen ist, wird somit auch dessen MAC-Adresse bekannt und diese wird auch in die FDB übernommen.
- **Der Sender** empfängt den ARP-Reply und trägt in seine lokale ARP-Table die MAC-Adresse des Empfängers ein. Danach beginnt er mit dem Senden der Datenpakete mit IP- und MAC-Adresse des Empfängers. Der Switch weiß über die Empfänger MAC-Adresse, auf welchem Port er diese Pakete senden soll und leitet sie entsprechend weiter.
- **Ist der** gewünschte Empfänger in einem anderen Netzsegment (z.B. anderes IP-Netz) beheimatet, so übernimmt ein Router in seiner Rolle als sogenanntes Default Gateway die Pakete und leitet sie in Richtung des angegebenen Zielnetzes weiter. In diesem Fall wird die Interface IP- und MAC-Adresse des Routers in die Switch-FDB übernommen.



Jeder Teilnehmer an einer Kommunikation hat somit eine eineindeutige Zuordnung aus IP-Adresse zu MAC-Adresse. Wird diese Kombination verändert oder werden Teile dieser Kombination auch von anderen Teilnehmern verwendet, so können Ausfälle und Fehlfunktionen auftreten, die den Datenfluss verändern und auch zum Erliegen bringen können.

Whitepaper: IP-MAC-Port-Binding (IMPB)

Das Böse schlägt zu

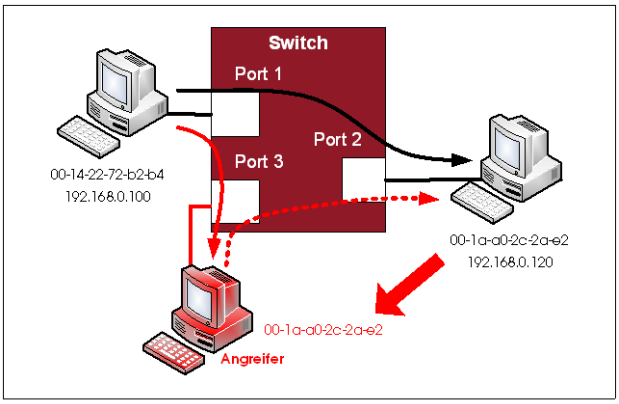
Es kann - muss aber nicht immer - der hinterhältige Bösewicht sein, der sich unautorisiert in den Besitz von Daten bringen möchte. Auch defekte oder falsch konfigurierte Endgeräte können den Datenverkehr zum Erliegen bringen. Konfiguriert man beispielsweise einen neuen Druckerserver im Netzwerk versehentlich mit der IP-Adresse des Routers oder meldet sich dieser Drucker anhand eines Fehlers mit der MAC-Adresse des Routers (Default Gateway), so wenden sich ab diesem Zeitpunkt alle Geräte an diesen Server, um in ein anderes Netzwerksegment zu gelangen. Der Druckerserver kann naturgemäß mit diesen Anfragen nichts anfangen und verwirft diese Daten. Ab diesem Zeitpunkt kommt der segmentübergreifende Verkehr komplett zum Erliegen.

Ein anderes Szenario stellt einen Angreifer dar, der bewusst den Datenverkehr zum Erliegen bringen möchte oder aber Interesse an den Datenpaketen und ihrem Inhalt zeigt. Zunächst einmal kann ein solcher Angreifer in ungeschützten Umgebungen mit einem ARP-Scan die aktuellen Zuordnungen von IP-Adressen zu MAC-Adressen herausfinden. Betreibt er dies passiv, dann bekommt er mit der Zeit die ARP-Requests der einzelnen Rechner mit, welche per Broadcast nach der MAC-Adresse ihres gewünschten Kommunikationspartners fragen. In diesem ARP Request stehen sowohl die IP-Adresse als auch die MAC-Adresse des Senders und der Angreifer kann diese Zuordnung speichern. Auch das Default Gateway (der Router) fragt von Zeit zu Zeit nach der MAC-Adresse von Geräten in diesem Segment, um an diese Verkehr von außerhalb zu senden. In diesem Fall kann ein Angreifer die IP/MAC Zuordnung des Default Gateways herauslesen und speichern. Ebenso ist es möglich, das Herausfinden von IP- und MAC-Adressen aktiv mit IP-Scans und ARP-Scans zu betreiben – allerdings werden diese Methoden schneller erkannt und entsprechende Gegenmaßnahmen können ergriffen werden.

Hat ein Angreifer ausreichend Daten gesammelt, so stehen ihm unterschiedliche Angriffsvarianten zur Auswahl:

- **ARP-Spoofing ohne Weiterleitung des Datenverkehrs**
  Dies bedeutet, der Angreifer schickt Datenpakete mit der MAC-Adresse des anzugreifenden Rechners. Dadurch wird der Datenverkehr, der eigentlich zu dem nun angegriffenen Rechner laufen sollte, zum Angreifer geleitet. Dieser sendet den Datenstrom nicht weiter. Der angegriffene Rechner bemerkt dies, da kein Datenverkehr mehr bei ihm ankommt.

- **ARP-Spoofing mit Weiterleitung des Datenverkehrs**
  Ebenso wie im vorherigen Fall schickt der Angreifer wieder Datenpakete mit der MAC-Adresse des anzugreifenden Rechners. Wieder wird der Datenverkehr, der eigentlich zu dem nun angegriffenen Rechner laufen sollte, zum Angreifer geleitet. Dieses Mal sendet dieser den Datenstrom aber weiter an den eigentlichen Zielrechner. Der Zielrechner bemerkt dadurch nicht den Eingriff durch den angreifenden Rechner. Der Angreifer ist somit in der Lage, unbemerkt den Datenverkehr mitzulesen.



- **Man-in-the-Middle Attacke**
  Diese Attacke ist die konsequente Fortführung des oben beschriebenen Angriffs mit der Weiterleitung des Datenverkehrs an den ursprünglichen Empfänger. Hierbei setzt der Angreifer sich in eine, ggf. auch verschlüsselte Kommunikation, um Daten gezielt zu verändern. Die Veränderung von vermeintlich sicheren, da verschlüsselten Daten, ist hierbei als besonders kritisch einzustufen, da sie vom angegriffenen User meist nicht zu erkennen ist.

Whitepaper: IP-MAC-Port-Binding (IMPB)

Gegenmaßnahmen

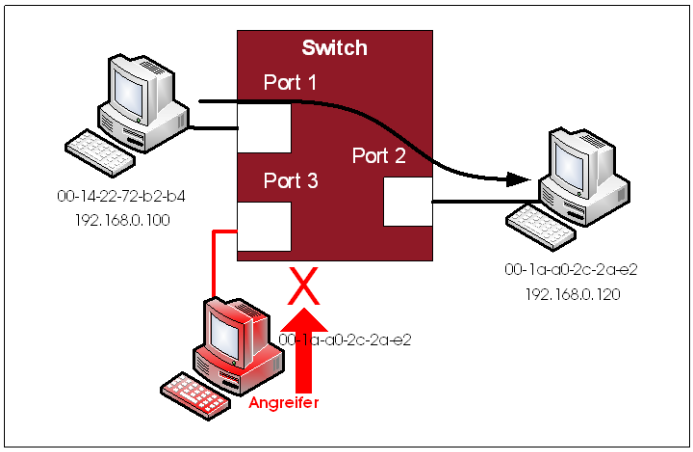
IP-MAC-Port-Binding verhindert, dass eine, wie zuvor beschriebene, bewusste oder unbewusste Veränderung der Zuordnung von IP zu MAC Adresse erfolgen kann.

Um überprüfen zu können, ob ein angeschlossenes Endgerät eine korrekte Kombination aus IP- und MAC-Adresse verwendet, muss zunächst einmal die erlaubte Zuordnung von IP- zu MAC-Adresse im Switch in der IMPB Database hinterlegt werden. Hierzu gibt es zwei unterschiedliche Möglichkeiten der Konfiguration in den D-Link xStack Switches:

- **Statisch über „Static IMP Entry“**
  Die korrekten Zuordnungen können statisch im Switch konfiguriert werden. Die nötigen Informationen (IP-Adresse, MAC-Adresse, Ports) können hierzu über das WEB-Interface oder das Command Line Interface (CLI per serieller Schnittstelle oder über Telnet/SSH) eingegeben werden. Ändert sich die Zuordnung, z.B. wegen dem Austausch einer defekten Netzwerkkarte, so müssen die entsprechenden Einträge im Switch angepasst werden.

- **Dynamisch über „DHCP snooping“**
  In Umgebungen mit dynamischer IP-Adressvergabe über DHCP ist eine statische Konfiguration des Switches mit einer fixen Zuordnung von IP- zu MAC-Adresse nicht realisierbar. Für diesen Fall ist die Konfiguration von IMPB mit DHCP snooping zu verwenden. Der Switch erkennt anhand der DHCP-Anfrage der Clients und der entsprechenden Antwort des Servers die IP-Adresse, ordnet sie der an dem Port anliegenden MAC-Adresse zu und trägt sie selbstständig in die IMPB Tabelle ein. Somit entfällt ein Großteil der administrativen Arbeit zur Pflege der Tabelle, welches sich insbesondere in großen Netzen positiv auswirkt.

Die eigentliche Überprüfung der gesammelten und in der IMPB Database hinterlegten Adress-Zuordnungen erfolgt nun entweder über das Scannen von ARP Broadcast Paketen (ARP Mode) oder über den Vergleich mit Access Listen (ACL Mode).



Im **ARP Mode**, dem Standardmode nach dem aktivieren von IMPB, werden eingehende ARP Anfragen für eine Überprüfung herangezogen. Stimmen die dort enthaltenen Source MAC- und IP-Adressen mit den konfigurierten überein, so wird ein entsprechender Eintrag mit „allowed“ in die L2 Forwarding Database (FDB) angelegt und der Verkehr zugelassen. Stimmt die in dem ARP Paket enthaltene Kombination aus MAC- und IP-Adresse nicht mit der in der IMPB hinterlegten überein, so wird ein entsprechender Eintrag in der FDB mit „drop“ angelegt und er Verkehr verworfen. Um den Switch durch diese Funktionalität nicht zusätzlich zu belasten, werden ausschließlich ARP Broadcasts zur Überprüfung herangezogen, welche sowieso von der Switch CPU verarbeitet werden müssen.

Im **ACL Mode** wird aus den Einträgen in der IMPB Tabelle automatisch eine Reihe von Access Listen erzeugt, welche für eine Überprüfung der eingehenden Datenpakete herangezogen werden. Diese Methode hat gegenüber dem ARP Mode den Vorteil, dass bereits ab dem ersten Paket eine Überprüfung erfolgen kann und nicht erst nach Erhalt des ersten ARP Broadcasts. Wird per Access Liste festgestellt, dass die MAC- IP-Adressen Kombination korrekt ist, wird der Verkehr weitergeleitet. Ist die Kombination nicht korrekt, so wird der entsprechende Datenverkehr verworfen. Der ACL Mode kann zusätzlich zum ARP Mode verwendet werden.

Whitepaper: IP-MAC-Port-Binding (IMPB)

Sicherer Anschluss ans Netz

Durch die Aktivierung von IMPB in den Switches im Etagen und Serverbereich kann die Stabilität des Netzwerks und die Zugriffssicherheit wesentlich erhöht werden. In Umgebungen mit dynamischer IP Adressenvergabe erfolgt eine weitgehend automatisierte Konfiguration des Netzes durch die DHCP-Snooping Funktionalität. IMPB muss einmalig im Switch und jeweils auf den gewünschten Access-Ports konfiguriert werden. Sollten Rechner oder Server mit fixen IP-Adressen versehen sein, so können diese komfortabel über das WEB-Interface konfiguriert werden.

Erkennt der Switch eine nicht authentifizierte MAC- IP-Adressen Kombination, so kann automatisch ein Log-Eintrag erzeugt werden, um diesen Vorfall zu dokumentieren und an einen Log-Server zu senden. Somit ist auch die Integration in Management Umgebung möglich, um eine zuverlässige Überwachung der Netzumgebung zu gewährleisten.

Sicherheitskonzept mit D-Link

IP-MAC-Port-Binding bildet zusammen mit weiteren, von D-Link in den xStack Switchen implementierten, Funktionen, wie zum Beispiel Loopback-Detection, DHCP-Server-Screening, Safeguard Engine und die Unterstützung von Microsoft NAP einen wichtigen Baustein zur Bildung eines Gesamtkonzepts für Sicherheit, Stabilität, Performance, Redundanz und Verwaltbarkeit in Ihrem Netzwerk.

Aktuelle Themen im Rahmen					
Sicherheit	**Stabilität**	**Performance**	**Redundanz**	**Verwaltbarkeit**	**D-Link Lösung**
	Loop Connections				**Loopback-Detection**
	Mehrere DHCP Server				**DHCP Server Screening**
	Wurm Ausbrüche				**SafeguardEngine**
Wurm Ausbrüche					**Zonedefense**
ARP Spoofing					**IMPB v3**
Man in the Middle Attack					**IMPB v3**
Grundsätzlich geschützter Netzwerkzugriff					**ACL Liste Web based Access (WAC) 802.1x**
Erweiterter Netzwerkzugriff mit Policies					**Microsoft NAP**
		P2P Abusing			**Flow based Bandwidth Control**
			Chassis übergreifende Redundanz		**RERP (DES-7200)**
			Stacking		**Stacking auch über Glasfaser**
		Bandbreiten-erhöhung			**Stacking**
Überwachung / Konfigurations-rollout	Überwachung	Überwachung	Überwachung / Konfiguration	Einfache Administration	**D-View 6**

Folgende Switch Serien unterstützen IP-MAC-Port-Binding:

- **DES-3010/18/26**
- **DES-3028/52**
- **DES-3528/52**
- **DES-3800**
- **DGS-3200**
- **DGS-3400**
- **DGS-3600**