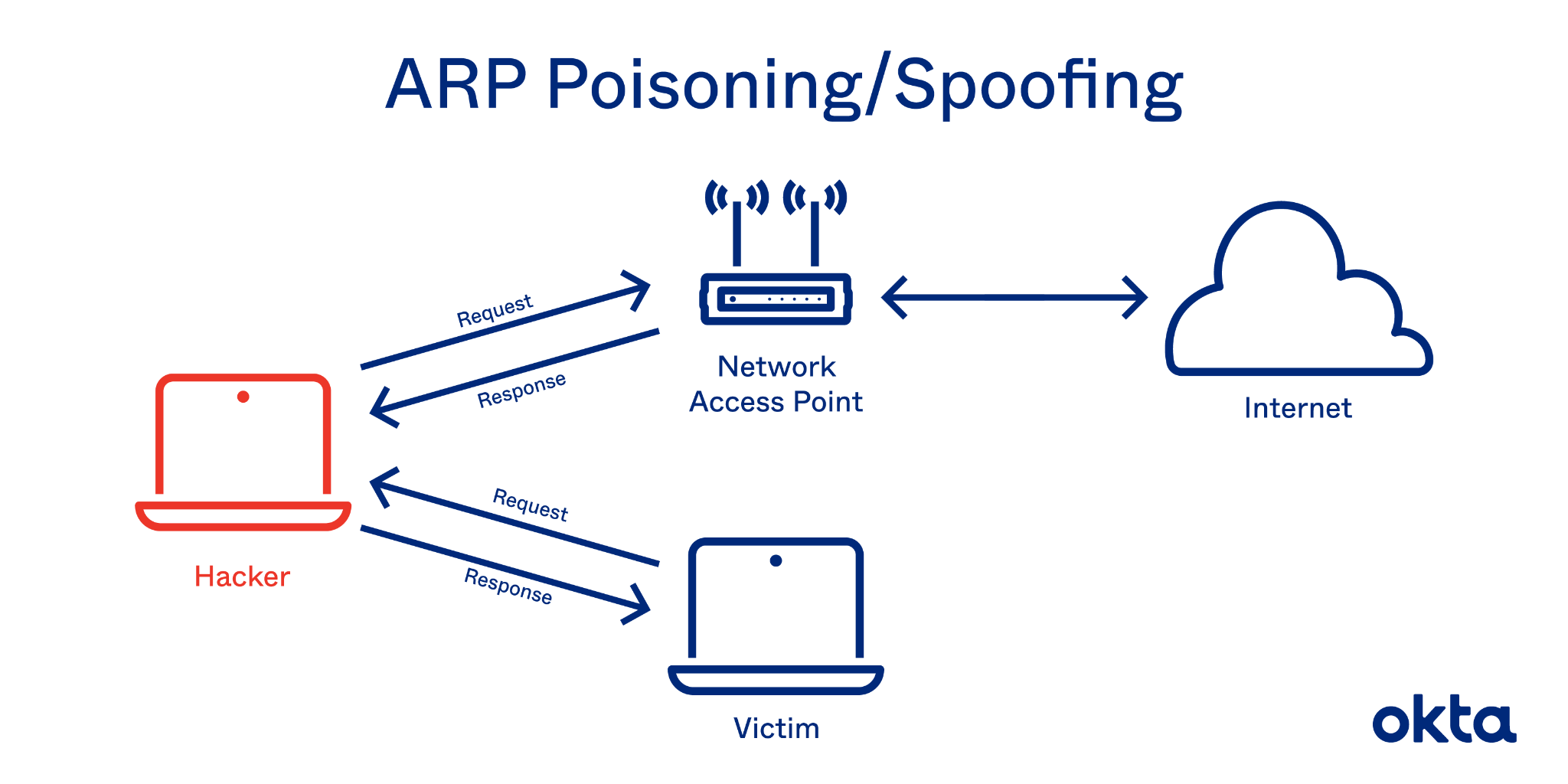
انواع حملات در لایه 2 /Osi

# حملات و تهدیدات لایه دو که منجر به نفوذ به سایر قسمت های شبکه و منابع شبکه می شود

# ARP Attacks

این پروتکل وجود دارد و آن اینست که هر کلاینت اجازه دارد یک ARP Reply را بدون اینکه کلاینتی ARP Request فرستاد بصورت برودکست ارسال کند در اصطلاح به این فریم ارسالی Gratuitous ARP گفته می شود و صرفا جهت معرفی آدرس مک کلاینت توسط خود کلاینت به سایر کلاینت ها استفاده می شود

پروتکل ARP توسط همه سیستم هایی که به یک شبکه اِترنت متصل هستند استفاده می شود. دستگاه ها از ARP برای پیدا کردن آدرس MAC لایه ۲ دستگاه مقصد و با استفاده از آدرس IP آنها استفاده می کنند. ARP به خودی خود نا‌امن است، زیرا دستگاه ها باید به جواب هایی که دریافت می کنند اطمینان کن.پروسه tree hand shake مهم است

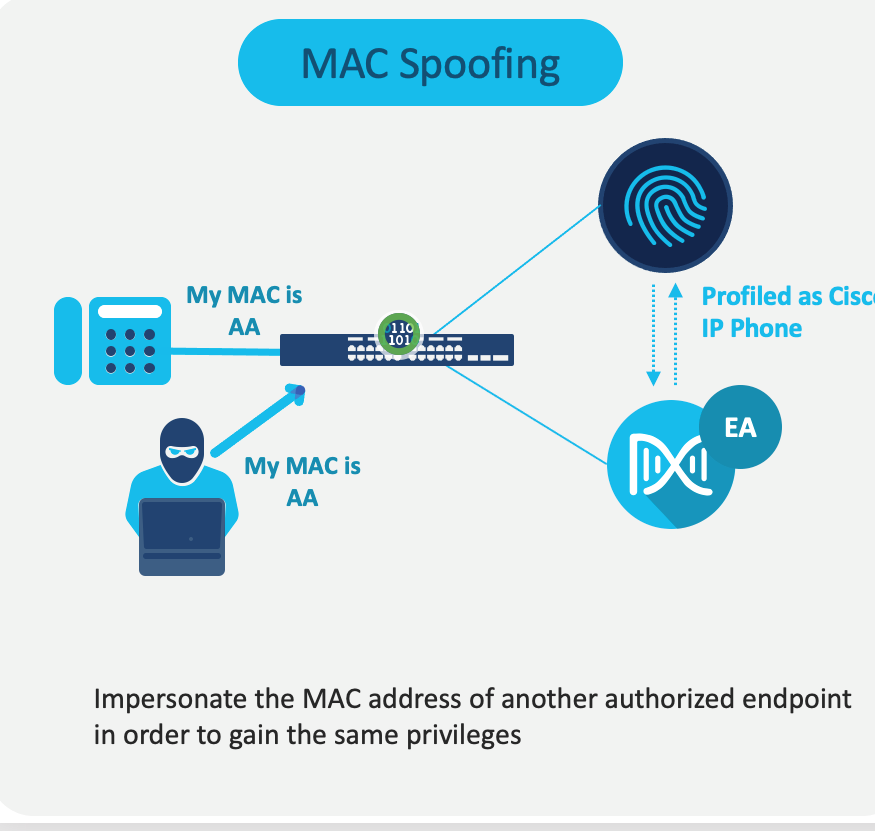


MAC Spoofing

# 

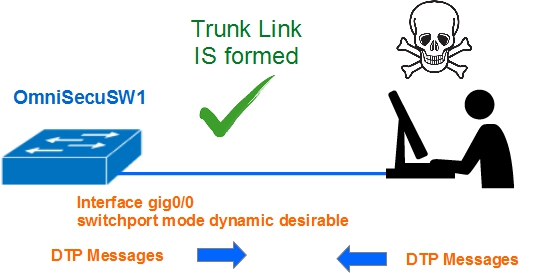
# صور کنید در شبکه ای یک هکر آدرس مک خود را به آدرس مک یکی از سیستم ها در شبکه تغییر دهد در این شرایط CAM table سوئیچ نیز تغییر می کند. با این عمل، ترافیک شبکه به آن سیستم خاص به سیستم هکر هدایت شده و در این صورت هکر می تواند ترافیک ارسالی به سیستم مورد نظر را بطور موقت شنود کند

به این ترتیب که هکر آدرس تمام سیستم‌های شبکه را که از طریق سوئیچ با هم در ارتباط هستند به دست می‌آورد. مک آدرس خود را در برابر سرور موجود در شبکه قرار می‌دهد و به سمت سوییچ ترافیک می‌فرستد



### Switch Spoofing

در این حمله هکر تلاش می کند یک سوئیچ اشتباه را به شبکه اضافه کند. اگر حمله موفق باشد ترافیک VLAN های مختلف از این سوییچ عبور خواهد کرد و امکان بازبینی و تغییرات اطلاعات را برای هکر ایجاد می کند



# 

## STP

(Spanning Tree Protocol (STP یک پروتکل مدیریت layer 2 link است. هدف اصلی STP اطمینان از عدم وجود حلقه های جریان داده در هنگامی که شبکه دارای مسیرهای اضافی است، می باشد. به طور کلی ، مسیرهای اضافی ساخته می شوند تا قابلیت اطمینان به شبکه را فراهم کنند. اما آن ها می توانند حلقه های مهلکی ایجاد کنند که می تواند منجر به حمله DoS در شبکه شود.

