MOTOTRBO Devices

Best Practices for

One-Time Software Activation

FEBRUARY 2023

MN008921A01-AC

Revision History

Revision	Date	Author	Description of Updates
Pre-Release	11/14/2021	Dan Zetzl	Initial Draft.
01.00	11/19/2021	Dan Zetzl	Release one after review comments incorporated.
01.01	3/23/2022	Dan Zetzl	Updated URLs in Table 2 for a typo in the Radio Central https entry and the IoT address.
01.02	1/25/2023		Added Russian language.

Table 1: Document Revision History

References

[1] Radio Management System Planner, MN004686A01

[2] Disable DNS Client-Side Caching, https://docs.microsoft.com/en-us/windows-server/networking/dns/troubleshoot/disable-dns-client-side-caching

Introduction

The MOTOTRBO Ion and R7 devices require a one-time activation to enable the software features and services that have been purchased with the device.

To simplify the one-time activation and to support devices without a display, the MOTOTRBO devices are shipped with a default Wi-Fi network profile. In addition to the one-time activation of the MOTOTRBO devices, customers using the Radio Management or the Radio Central application may choose to use the same Wi-Fi network for a zero touch enrollment of the device into those applications.

This document provides best practice recommendations related to the security and operation of the Wi-Fi network used for one-time activation.

Best Practice Recommendations for Wi-Fi Network

IP Address Assignment

MOTOTRBO devices are configured, by default, to obtain an IP address via DHCP. The following recommendations are provided to ensure that the pool of IP addresses used by the DHCP service is not depleted during bulk programming of devices.

1. It is recommended that you configure your DHCP server to use short DHCP lease times. This allows you to reuse the same IP addresses as batches of radios are completed.
2. It is recommended that you configure your DHCP server with a sufficient quantity of IP addresses to provide addresses to the number of MOTOTRBO devices you will program simultaneously during bulk provisioning plus the other devices that will be on the network such as the Radio Management Device Programmer. Note: You need to take into account when the DHCP lease, discussed above, will expire to allow you to reuse those IP addresses.

MOTOTRBO Device Discovery (Radio Management)

MOTOTRBO devices are configured, by default, to send a mDNS-SD[1] message when connecting to a Wi-Fi network and every 90 seconds thereafter. The Radio Management Device Programmer also sends mDNS-SD messages. The following recommendations are provided to enable the Radio Management software to automatically discover and read MOTOTRBO devices without any action required by the user.

1. The UDP port number for DNS-SD is port 5353. The IPv4 address is 224.0.0.251. The network firewall rules must allow this port number and broadcast for the service to operate.
2. The MOTOTRBO device and Radio Management Device Programmer must be on the same network segment or the multicast traffic must be forwarded between network segments (for example, using a VLAN[2]). Details on how to configure your network equipment to forward multicast traffic can usually be found in your network equipment manufacturer's product literature.

[1] Multicast Domain Name Service Service Discovery
[2] Virtual Local Area Network

Note: The service discovery destination can be updated to an unicast IP or hostname using the Radio Management software.

Please refer to the Radio Management System Planner for more details.

Network Time Server Availability

MOTOTRBO devices are configured, by default, to obtain the current time via the NTP[3].

Primary NTP Server	pool.ntp.org
Secondary NTP Server	time.google.com

MOTOTRBO devices enrolling for certificates using SCEP[4] require an accurate time as part of the CSR[5]. An accurate time is required for a reliable connection to the Radio Central cloud service.

Wi-Fi Channel Usage

All MOTOTRBO devices support Wi-Fi Generation 1 (802.11b), Wi-Fi Generation 3 (802.11g), and Wi-Fi Generation 4 (802.11n).

MOTOTRBO Ion and MOTOTRBO R7 also support Wi-Fi Generation 5 (802.11ac) and MOTOTRBO Ion supports Wi-Fi Generation 6 (802.11ax) as well.

It is a best practice to select non-overlapping Wi-Fi channels to maximize throughput on the network. Specifically, this recommendation applies to Wi-Fi access points with overlapping coverage. This avoids adjacent channel interference between the Wi-Fi access points.

[3] Network Time Protocol
[4] Simple Certificate Enrollment Protocol
[5] Certificate Signing Request

In the 2.4 GHz spectrum, it is recommended that you select channels 1, 6 and 11 for Wi-Fi access points with overlapping coverage. Note: Other sources of interference such as microwave ovens may interfere with network performance.

In the 5 GHz spectrum, there are 24 non-overlapping channels (36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161 and 165). In addition, there are less sources of interference. By default, some Wi-Fi access points will “steer” devices to 5 GHz by slowing responses to 2.4 GHz.

The use of multiple access points to increase the total bandwidth available should be considered when bulk provisioning.

Best Practice Recommendations for Security

The use of an enrollment network to separate untrusted clients from the corporate network is a recommended best practice. In the case of MOTOTRBO devices, the initial enrollment network is enabled by default.

Wi-Fi Personal Network Pre-Shared Key (PSK) SSID - MOTOTRBO
Passphrase: Radio Management

Limit Physical Access to Enrollment Network

It is a recommended best practice to limit physical access to the Wi-Fi coverage area of the enrollment network to trusted individuals.

Change Default Wi-Fi Network Settings

It is a recommended best practice to update the Wi-Fi network and passphrase to something other than the default value.

Enterprise Wi-Fi Networks

From a security standpoint, the use of Wi-Fi Enterprise networks provide several advantages when compared with Wi-Fi personal networks. The advantages include the ability to disable network access on an individual device basis without impacting the other devices on the network, that traffic is uniquely encrypted between the Wi-Fi access point and each device, and

the ability to update the credentials used for the encryption using standard certificate management practices. MOTOTRBO devices support both Wi-Fi Personal and Wi-Fi Enterprise networks.

Use an Access Control List

An Access Control List (ACL) can be used to restrict clients to only the enrollment network and the servers and services required to activate the device.

Application or Service	Hostname	Port	Direction	Protocol
NTP	Pool.ntp.org time.google.com	123	Outbound	UDP
DHCP	n/a (network provided)	67 68	Outbound Inbound	UDP
DNS	n/a (network provided)	53	Outbound	TCP & UDP
Certificate Management	https://devicecertmgmt-cmf21.motsolpki.com https://devicecertmgmt-cmf21.motsolpki.com	49682 49684	Outbound	https
Radio Central	locator.radiocentral.motorolasolutions.com	443	Outbound	https
Radio Central	Api-us.radiocentral.motorolasolutions.com Api-au.radiocentral.motorolasolutions.com	443	Outbound	https
Radio Central	Usp9rmstorage.blob.core.windows.net aup9rmstorage.blob.core.windows.net	443	Outbound	https

IoT Service	global.azure-devices-provisioning.net	443	Outbound	https
IoT Service	iotcs-hub-us.azure-devices.net	8883	Outbound Inbound	MQTT

Table 2: Device Network Connections for One-Time Activation

Historique des révisions

Révision	Date	Auteur	Description des mises à jour
Préversion	14 novembre 2021	Dan Zetzl	Ébauche initiale.
01.00	19 novembre 2021	Dan Zetzl	Première version après intégration des commentaires issus de la révision.
01.01	23 mars 2022	Dan Zetzl	Mise à jour d'adresses URL dans le tableau 2 pour corriger une coquille dans l'entrée https de Radio Central et dans l'adresse du service IdO.
01.02	25 janvier 2023		Ajout du russe.

Tableau 1 : Historique des révisions apportées au document

Références

[1] Planificateur du système de Gestion radio, MN004686A01

[2] Désactivation de la mise en cache côté client DNS, https://docs.microsoft.com/fr-ca/windows-server/networking/dns/troubleshoot/disable-dns-client-side-caching

Introduction

Les appareils MOTOTRBO Ion et R7 requièrent une activation unique qui permet la mise en marche des fonctions logicielles et des services qui ont été achetés avec l'appareil.

Afin de simplifier cette activation unique et de prendre en charge les appareils sans écran, les appareils MOTOTRBO sont expédiés avec un profil de réseau Wi-Fi établi par défaut. En plus de l'activation unique des appareils MOTOTRBO, les clients qui emploient la Gestion radio ou l'application Radio Central peuvent choisir d'utiliser le même réseau Wi-Fi pour une inscription de l'appareil sans intervention dans ces applications.

Ce document présente des pratiques exemplaires recommandées liées à la sécurité et au fonctionnement du réseau Wi-Fi utilisé pour l'activation unique.

Pratiques exemplaires recommandées pour le réseau Wi-Fi

Affectation de l'adresse IP

Les appareils MOTOTRBO sont configurés par défaut pour obtenir une adresse IP via DHCP (Dynamic Host Configuration Protocol). Les recommandations qui suivent sont fournies pour s'assurer que le bassin d'adresses IP utilisé par le service DHCP ne s'épuise pas pendant la programmation en lot d'appareils.

1. Nous vous recommandons de configurer votre serveur DHCP de façon à ce qu'il utilise de courtes durées de bail DHCP. Ceci vous permet de réutiliser les mêmes adresses IP au fur et à mesure que des lots de radios sont achevés.
2. Nous vous recommandons de configurer votre serveur DHCP avec une quantité suffisante d'adresses IP pour fournir des adresses au nombre d'appareils MOTOTRBO que vous programmerez simultanément pendant l'approvisionnement en lot, en plus des autres appareils qui seront sur le réseau, comme le programmeur d'appareil de Gestion radio. Remarque : Vous devez tenir compte du moment où le bail DHCP mentionné ci-dessus vient à échéance afin de pouvoir réutiliser ces adresses IP.

Découverte de l'appareil MOTOTRBO (Gestion radio)

Les appareils MOTOTRBO sont configurés par défaut pour envoyer un message mDNS-SD[1] lorsqu'ils se connectent à un réseau Wi-Fi et à toutes les 90 secondes par la suite. Le programmeur d'appareil de Gestion radio envoie aussi des messages mDNS-SD. Nous vous fournissons les recommandations suivantes pour permettre au logiciel de Gestion radio de découvrir et de lire automatiquement les appareils MOTOTRBO sans que l'utilisateur ait à faire quoi que ce soit.

1. Le numéro de port UDP pour DNS-SD est le port 5353. L'adresse IPv4 est 224.0.0.251. Les règles du pare-feu de réseau doivent autoriser ce numéro de port et cette diffusion pour que le service fonctionne.
2. L'appareil MOTOTRBO et le programmeur d'appareil de Gestion radio doivent être sur le même segment de réseau ou le trafic de multidiffusion doit être transféré entre segments de réseau (par exemple, avec un réseau VLAN[2]). Les détails de configuration de votre équipement de réseau pour transférer le trafic de multidiffusion se trouvent normalement dans les documents du fabricant qui accompagnent votre équipement de réseau.

[1] Découverte du service de nom du domaine de multidiffusion
[2] Réseau local virtuel

Remarque : La destination de découverte du service peut être mise à jour à une adresse IP unicast ou à un nom d'hôte à l'aide du logiciel de Gestion radio.

Veuillez consulter le planificateur du système de Gestion radio pour obtenir plus de détails.

Disponibilité du serveur de synchronisation de réseaux

Les appareils MOTOTRBO sont configurés par défaut pour obtenir l'heure actuelle par l'entremise du serveur NTP[3].

Serveur NTP principal	pool.ntp.org
Serveur NTP secondaire	time.google.com

Les appareils MOTOTRBO s'inscrivant pour des certificats à l'aide de SCEP[4] requièrent l'heure précise dans le cadre du CSR[5]. L'heure précise est requise pour établir une connexion digne de confiance au service infonuagique de Radio Central.

Utilisation du canal Wi-Fi

Tous les appareils MOTOTRBO prennent en charge le Wi-Fi Génération 1 (802.11b), le Wi-Fi Génération 3 (802.11g), et le Wi-Fi Génération 4 (802.11n).

Les appareils MOTOTRBO Ion et MOTOTRBO R7 prennent aussi en charge le Wi-Fi Génération 5 (802.11ac) et l'appareil MOTOTRBO Ion prend en charge le Wi-Fi Génération 6 (802.11ax) également.

Une pratique exemplaire consiste à choisir des canaux Wi-Fi qui ne se chevauchent pas afin de maximiser le débit du réseau. Plus précisément, cette recommandation s'applique aux points d'accès Wi-Fi dont la couverture se chevauche. Ainsi, l'interférence entre canaux adjacents est évitée entre les points d'accès Wi-Fi.

[3] Network Time Protocol
[4] Simple Certificate Enrollment Protocol
[5] Certificate Signing Request

Dans le spectre des 2,4 GHz, il est recommandé de choisir les canaux 1, 6 et 11 pour les points d'accès Wi-Fi dont la couverture se chevauche. Remarque : D'autres sources d'interférence, comme les fours à micro-ondes, peuvent nuire au rendement du réseau.

Dans le spectre de 5 GHz, il existe 24 canaux qui ne se chevauchent pas (36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161 et 165). De plus, il comporte moins de sources d'interférence. Par défaut, certains points d'accès « poussent » les appareils vers le 5 GHz en ralentissant la réaction du spectre des 2,4 GHz.

Vous devriez envisager d'utiliser des points d'accès multiples pour avoir plus de bande passante à votre disposition pour l'approvisionnement en lot.

Pratiques exemplaires recommandées en matière de sécurité

L'utilisation d'un réseau d'inscription pour séparer les clients non sûrs du réseau d'entreprise est une pratique exemplaire recommandée. Pour les appareils MOTOTRBO, le réseau d'inscription initiale est activé par défaut.

Clé prépartagée du réseau Wi-Fi personnel (PSK) SSID – MOTOTRBO
Phrase de passe : Radio Management

Limitation de l'accès physique au réseau d'inscription

L'une des pratiques exemplaires recommandées est de limiter l'accès physique à la zone de couverture Wi-Fi du réseau d'inscription aux personnes dignes de confiance.

Changement des paramètres de réseau par défaut du réseau Wi-Fi

Une pratique exemplaire recommandée est de mettre à jour le réseau Wi-Fi et sa phrase de passe à autre chose que leurs valeurs par défaut.

Réseaux Wi-Fi d'entreprise

Sur le plan de la sécurité, l'utilisation de réseaux Wi-Fi d'entreprise présente de nombreux avantages par rapport à l'utilisation de réseaux Wi-Fi personnels. Parmi ces avantages, mentionnons la possibilité de désactiver l'accès au réseau selon l'appareil individuel sans avoir d'incidence sur les autres appareils dans le réseau, le trafic à chiffrement unique entre le point d'accès Wi-Fi et chaque appareil, et la possibilité de mettre à jour les identifiants utilisés pour le chiffrement à l'aide de pratiques normalisées de gestion des certificats. Les appareils MOTOTRBO prennent en charge les réseaux Wi-Fi personnels et les réseaux Wi-Fi d'entreprise.

Utilisation d'une liste de contrôle d'accès

Une liste de contrôle d'accès (ACL) peut être utilisée pour limiter les clients au réseau d'inscription seulement et aux serveurs et services requis pour l'activation de l'appareil.

Application ou service	Nom d'hôte	Port	Direction	Protocole
NTP	Pool.ntp.org time.google.com	123	Sortante	UDP
DHCP	s. o. (fourni par le réseau)	67 68	Sortante Entrante	UDP
DNS	s. o. (fourni par le réseau)	53	Sortante	TCP et UDP
Gestion des certificats	https://devicecertmgmt-cmf21.motsolpki.com https://devicecertmgmt-cmf21.motsolpki.com	49682 49684	Sortante	https
Radio Central	locator.radiocentral.motorolasolutions.com	443	Sortante	https
Radio Central	Api-us.radiocentral.motorolasolutions.com Api-au.radiocentral.motorolasolutions.com	443	Sortante	https
Radio Central	Usp9rmstorage.blob.core.windows.net aup9rmstorage.blob.core.windows.net	443	Sortante	https
Service IdO	global.azure-devices-provisioning.net	443	Sortante	https
Service IdO	iotcs-hub-us.azure-devices.net	8883	Sortante Entrante	MQTT

Tableau 2 : Connexions réseau de l'appareil pour l'activation unique

Historial de revisiones

Revisión	Fecha	Autor	Descripción de las actualizaciones
Versión preliminar	14/11/21	Dan Zetzl	Borrador inicial.
01.00	19/11/21	Dan Zetzl	Primera versión después de incorporar los comentarios de la revisión.
01.01	23/03/22	Dan Zetzl	Se actualizaron las URL en la Tabla 2 debido a un error tipográfico en la entrada https de Radio Central y en la dirección de IoT.
01.02	25/01/23		Se agregó el idioma ruso.

Tabla 1: Historial de revisiones del documento

Referencias

[1] Radio Management System Planner, MN004686A01

[2] Desactivar el almacenamiento en caché del lado cliente DNS: https://docs.microsoft.com/es-mx/windows-server/networking/dns/troubleshoot/disable-dns-client-side-caching

Introducción

Los dispositivos MOTOTRBO Ion y R7 requieren una activación única a fin de habilitar las funciones y los servicios del software que se han adquirido con el dispositivo.

Para simplificar la activación única y admitir dispositivos sin pantalla, los dispositivos MOTOTRBO se envían con un perfil de red Wi-Fi predeterminado. Además de la activación única de los dispositivos MOTOTRBO, los clientes que utilizan Radio Management o la aplicación Radio Central pueden elegir utilizar la misma red Wi-Fi para realizar una inscripción sin intervención del dispositivo en esas aplicaciones.

En este documento, se proporcionan prácticas recomendadas relacionadas con la seguridad y el funcionamiento de la red Wi-Fi que se utiliza para la activación única.

Prácticas recomendadas para redes Wi-Fi

Asignación de la dirección IP

Los dispositivos MOTOTRBO se configuran, de forma predeterminada, para obtener una dirección IP a través de DHCP. Se proporcionan las siguientes recomendaciones para garantizar que el grupo de direcciones IP que el servicio DHCP utiliza no se agote durante la programación masiva de dispositivos.

1. Se recomienda configurar el servidor DHCP para que utilice tiempos de concesión de DHCP breves. Esto permitirá volver a utilizar las mismas direcciones IP a medida que se completen los lotes de radios.
2. Se recomienda que configure su servidor DHCP con una cantidad suficiente de direcciones IP a fin de proporcionar direcciones a la cantidad de dispositivos MOTOTRBO que programará simultáneamente durante el aprovisionamiento masivo, además de los otros dispositivos que estarán en la red, como Radio Management Device Programmer. Nota: Debe tener en cuenta cuándo se vencerá la concesión de DHCP, que se mencionó anteriormente, para poder volver a utilizar esas direcciones IP.

Detección de dispositivos MOTOTRBO (Radio Management)

Los dispositivos MOTOTRBO están configurados, de forma predeterminada, para enviar un mensaje mDNS-SD[1] cuando se conectan a una red Wi-Fi y cada 90 segundos a partir de entonces. Radio Management Device Programmer también envía mensajes mDNS-SD. Se proporcionan las siguientes recomendaciones para permitir que el software Radio Management detecte y lea automáticamente dispositivos MOTOTRBO sin necesidad de que el usuario realice ninguna acción.

1. El número de puerto UDP para DNS-SD es el 5353. La dirección IPv4 es 224.0.0.251. Las reglas del firewall de red deben permitir este número de puerto y transmisión para que el servicio funcione.
2. El dispositivo MOTOTRBO y Radio Management Device Programmer deben estar en el mismo segmento de red o el tráfico de multidifusión debe reenviarse entre segmentos de red (por ejemplo, mediante una VLAN[2]). Los detalles sobre cómo configurar su equipo de red para reenviar el tráfico de multidifusión generalmente se pueden encontrar en la documentación del producto del fabricante del equipo de red.

[1] Detección de servicios del servicio de nombres de dominio de multidifusión
[2] Red de área local virtual

Nota: El destino de la detección de servicios se puede actualizar a una dirección IP o a un nombre de host de monodifusión mediante el software Radio Management.

Consulte Radio Management System Planner para obtener más información.

Disponibilidad del servidor de hora de la red

Los dispositivos MOTOTRBO se configuran, de forma predeterminada, para obtener la hora actual a través del NTP[3].

Servidor NTP principal	pool.ntp.org
Servidor NTP secundario	time.google.com

Los dispositivos MOTOTRBO que se inscriben para obtener certificados mediante SCEP[4] requieren una hora exacta como parte del CSR[5]. Se requiere una hora precisa para una conexión confiable con el servicio de nube de Radio Central.

Uso del canal Wi-Fi

Todos los dispositivos MOTOTRBO admiten Wi-Fi de primera generación (802.11b), Wi-Fi de tercera generación (802.11g) y Wi-Fi de cuarta generación (802.11n).

MOTOTRBO Ion y MOTOTRBO R7 también son compatibles con Wi-Fi de quinta generación (802.11ac), y MOTOTRBO Ion también admite Wi-Fi de sexta generación (802.11ax).

Una práctica recomendada es seleccionar canales Wi-Fi no superpuestos para maximizar el rendimiento en la red. Específicamente, esta recomendación se aplica a los puntos de acceso Wi-Fi con cobertura superpuesta. Esto evita la interferencia de canales adyacentes entre los puntos de acceso Wi-Fi.

[3] Network Time Protocol
[4] Simple Certificate Enrollment Protocol
[5] Certificate Signing Request

En el espectro de 2,4 GHz, se recomienda seleccionar los canales 1, 6 y 11 para los puntos de acceso Wi-Fi con cobertura superpuesta. Nota: Otras fuentes de interferencia, como hornos de microondas, pueden interferir en el rendimiento de la red.

En el espectro de 5 GHz, hay 24 canales no superpuestos (36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161 y 165). Además, hay menos fuentes de interferencia. De forma predeterminada, algunos puntos de acceso Wi-Fi “direccionan” los dispositivos a la conexión 5 GHz disminuyendo las respuestas a 2,4 GHz.

Se deberá considerar el uso de múltiples puntos de acceso para aumentar el ancho de banda total disponible cuando se realice un aprovisionamiento masivo.

Prácticas recomendadas de seguridad

Una práctica recomendada es utilizar una red de inscripción para separar clientes no confiables de la red corporativa. En el caso de los dispositivos MOTOTRBO, la red de inscripción inicial está activada de forma predeterminada.

SSID de clave previamente compartida (PSK) de red Wi-Fi personal: MOTOTRBO
Frase de contraseña: Radio Management

Limitación del acceso físico a la red de inscripción

Una práctica recomendada es limitar el acceso físico al área de cobertura Wi-Fi de la red de inscripción a personas de confianza.

Cambio de la configuración de red Wi-Fi predeterminada

Una práctica recomendada es actualizar la red Wi-Fi y la frase de contraseña a algo distinto del valor predeterminado.

Redes Wi-Fi empresariales

Desde el punto de vista de la seguridad, el uso de redes Wi-Fi empresariales ofrece varias ventajas en comparación con redes Wi-Fi personales. Las ventajas incluyen la capacidad de desactivar el acceso a la red en un dispositivo individual sin afectar a otros dispositivos de la red, que el tráfico se encripte de manera única entre el punto de acceso Wi-Fi y cada dispositivo, y la capacidad de actualizar las credenciales utilizadas para el encryption mediante prácticas estándar de administración de certificados. Los dispositivos MOTOTRBO admiten redes Wi-Fi personales y empresariales.

Uso de una lista de control de acceso

Se puede utilizar una lista de control de acceso (ACL) para restringir a los clientes solo a la red de inscripción y a los servidores y servicios necesarios para activar el dispositivo.

Aplicación o servicio	Nombre de host	destino	Dirección	Protocolo
NTP	Pool.ntp.org time.google.com	123	Saliente	UDP
DHCP	n/a (red proporcionada)	67 68	Saliente Entrante	UDP
DNS	n/a (red proporcionada)	53	Saliente	TCP y UDP
Administración de certificados	https://devicecertmgmt-cmf21.motsolpki.com https://devicecertmgmt-cmf21.motsolpki.com	49682 49684	Saliente	https
Radio Central	locator.radiocentral.motorolasolutions.com	443	Saliente	https
Radio Central	Api-us.radiocentral.motorolasolutions.com Api-au.radiocentral.motorolasolutions.com	443	Saliente	https
Radio Central	Usp9rmstorage.blob.core.windows.net aup9rmstorage.blob.core.windows.net	443	Saliente	https
Servicio de IoT	global.azure-devices-provisioning.net	443	Saliente	https
Servicio de IoT	iotcs-hub-us.azure-devices.net	8883	Saliente Entrante	MQTT

Tabla 2: Conexiones de red del dispositivo para la activación única

Histórico de revisões

Revisão	Data	Autor	Descrição das atualizações
Pré-Lançamento	14 de novembro de 2021	Dan Zetzl	Rascunho inicial.
01.00	19 de novembro de 2021	Dan Zetzl	Versão um após comentários de revisão incluídos.
01.01	23/03/2022	Dan Zetzl	URLs atualizados na Tabela 2 para corrigir um erro de digitação na entrada https do RadioCentral e no endereço IoT.
01.02	25/01/2023		Idioma russo adicionado.

Tabela 1: Histórico de revisão do documento

Referências

[1] Planejador do sistema de gerenciamento do rádio, MN004686A01

[2] Desativar cache no lado do cliente DNS
https://docs.microsoft.com/en-us/windows-server/networking/dns/troubleshoot/disable-dns-client-side-caching

Introdução

Os dispositivos MOTOTRBO Ion e R7 exigem uma ativação única para habilitar os recursos e serviços do software adquiridos com o dispositivo.

A fim de simplificar a ativação única e oferecer suporte a dispositivos sem monitor, os dispositivos MOTOTRBO são fornecidos com um perfil de rede Wi-Fi padrão. Além da ativação única dos dispositivos MOTOTRBO, os clientes que usam os aplicativos do Gerenciamento do rádio ou RadioCentral podem optar por usar a mesma rede Wi-Fi para um registro sem toque do dispositivo nesses aplicativos.

Este documento oferece recomendações de práticas de segurança e operação da rede Wi-Fi usada para a ativação única.

Práticas recomendadas para rede Wi-Fi

Atribuição de endereço IP

Como padrão, os dispositivos MOTOTRBO são configurados para obter um endereço IP via DHCP. As recomendações a seguir visam garantir que o pool de endereços IP usados pelo serviço DHCP não se esgote durante a programação em massa de dispositivos.

1. É recomendável configurar o servidor DHCP para usar tempos curtos de concessão de DHCP. Isso permite reutilizar os mesmos endereços IP conforme os lotes de rádios são concluídos.
2. É recomendável configurar seu servidor DHCP com uma quantidade suficiente de endereços IP, a fim de fornecer endereços para o número de dispositivos MOTOTRBO a serem programados simultaneamente durante o provisionamento em massa, além dos outros dispositivos que estarão na rede, como o Programador do dispositivo de gerenciamento do rádio. Observação: é preciso considerar quando a concessão de DHCP discutida acima expirará, permitindo a reutilização dos endereços IP.

MOTOTRBO Device Discovery (Gerenciamento do rádio)

Por padrão, os dispositivos MOTOTRBO são configurados para enviar uma mensagem mDNS-SD[1] quando se conectam a uma rede Wi-Fi e a cada 90 segundos posteriormente. O Programador do dispositivo do Gerenciamento do rádio também envia mensagens mDNS-SD. As recomendações a seguir permitem que o software de Gerenciamento do rádio detecte e leia automaticamente os dispositivos MOTOTRBO sem qualquer ação exigida pelo usuário.

1. O número da porta UDP para DNS-SD é a porta 5353. O endereço IPv4 é 224.0.0.251. As regras de firewall de rede devem permitir esse número de porta e difusão para que o serviço funcione.
2. O dispositivo MOTOTRBO e o Programador do dispositivo de Gerenciamento do rádio devem estar no mesmo segmento de rede ou o tráfego multicast deve ser encaminhado entre os segmentos de rede (por exemplo, através de uma VLAN[2]). Os detalhes sobre como configurar o equipamento de rede para encaminhar o tráfego multicast geralmente podem ser encontrados na literatura do produto do fabricante do equipamento de rede.

[1] Descoberta de serviço de nome de domínio Multicast
[2] Virtual Local Area Network (rede de área local virtual)

Observação: o destino da descoberta de serviço pode ser atualizado para um IP ou nome de host unicast com o software Radio Management.

Consulte o Planejador de sistema de Gerenciamento do rádio para mais detalhes.

Disponibilidade do servidor de horário da rede

Por padrão, os dispositivos MOTOTRBO são configurados para obter a hora atual por meio de NTP[3].

Servidor NTP Primário	pool.ntp.org
Servidor NTP Secundário	time.google.com

Os dispositivos MOTOTRBO que se inscrevem para certificados usando SCEP[4] requerem um tempo preciso como parte do CSR[5]. Um horário preciso é necessário para uma conexão confiável com o serviço de nuvem do RadioCentral.

Uso de canal Wi-Fi

Todos os dispositivos MOTOTRBO são compatíveis com Wi-Fi Geração 1 (802,11b), Wi-Fi Geração 3 (802,11g) e Wi-Fi Geração 4 (802,11n).

O MOTOTRBO Ion e o MOTOTRBO R7 também são compatíveis com Wi-Fi Geração 5 (802,11ac) e o MOTOTRBO Ion também é compatível com Wi-Fi Geração 6 (802,11ax).

É uma prática recomendada selecionar canais Wi-Fi sem sobreposição, a fim de maximizar a taxa de transferência na rede. Esta recomendação se aplica especificamente a pontos de acesso Wi-Fi com sobreposição de cobertura. Isso evita interferência de canal adjacente entre os pontos de acesso Wi-Fi.

[3] Network Time Protocol
[4] Simple Certificate Enrollment Protocol
[5] Certificate Signing Request

No espectro de 2,4 GHz, é recomendável selecionar os canais 1, 6 e 11 para pontos de acesso Wi-Fi com sobreposição de cobertura. Nota: outras fontes de interferência, como fornos de micro-ondas, podem interferir no desempenho da rede.

No espectro de 5 GHz, há 24 canais sem sobreposição (36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161 e 165). Além disso, há menos fontes de interferência. Por padrão, alguns pontos de acesso Wi-Fi "direcionam" os dispositivos para 5 GHz, retardando as respostas para 2,4 GHz.

O uso de vários pontos de acesso para aumentar a largura de banda total disponível deve ser considerado durante o provisionamento em massa.

Práticas recomendadas de segurança

O uso de uma rede de inscrição para separar clientes não confiáveis da rede corporativa é uma prática recomendada. No caso de dispositivos MOTOTRBO, a rede de inscrição inicial é ativada por padrão.

SSID de chave pré-compartilhada (PSK, Pre-Shared Key) da rede pessoal Wi-Fi - MOTOTRBO
Senha: Radio Management

Limite o acesso físico à rede de registro

É uma prática recomendada limitar o acesso físico à área de cobertura Wi-Fi da rede de inscrição a indivíduos confiáveis.

Altere as configurações de rede Wi-Fi padrão

É uma prática recomendada atualizar a rede Wi-Fi e a senha para algo diferente do valor padrão.

Redes de Wi-Fi comerciais

Do ponto de vista da segurança, o uso de redes Wi-Fi comerciais oferece várias vantagens em comparação com redes Wi-Fi pessoais. As vantagens incluem a capacidade de desativar o acesso à rede em um dispositivo sem afetar os outros dispositivos na rede; o tráfego é criptografado exclusivamente entre o ponto de acesso Wi-Fi e cada dispositivo; e a capacidade de atualizar as credenciais usadas para a criptografia usando práticas padrão de gerenciamento de certificados. Os dispositivos MOTOTRBO são compatíveis com redes de Wi-Fi pessoais e comerciais.

Use uma lista de controle de acesso

Uma lista de controle de acesso, ou ACL (Access Control List), pode ser usada para restringir clientes somente à rede de inscrição e aos servidores e serviços necessários para ativar o dispositivo.

Aplicativo ou Serviço	Nome do host	Porta	Direção	Protocolo
NTP	Pool.ntp.org time.google.com	123	Saída	UDP
DHCP	n/d (rede fornecida)	67 68	Saída Entrada	UDP
DNS	n/d (rede fornecida)	53	Saída	TCP & UDP
Gerenciamento de certificado	https://devicecertmgmt-cmf21.motsolpki.com https://devicecertmgmt-cmf21.motsolpki.com	49682 49684	Saída	https
RadioCentral	locator.radiocentral.motorolasolutions.com	443	Saída	https
RadioCentral	Api-us.radiocentral.motorolasolutions.com Api-au.radiocentral.motorolasolutions.com	443	Saída	https
RadioCentral	Usp9rmstorage.blob.core.windows.net aup9rmstorage.blob.core.windows.net	443	Saída	https
Serviço de IoT	global.azure-devices-provisioning.net	443	Saída	https
Serviço de IoT	iotcs-hub-us.azure-devices.net	8883	Saída Entrada	MQTT

Tabela 2: conexões de rede do dispositivo para ativação única

修订历史记录

修订版	日期	作者	更新说明
发行前版本	2021 年 11 月 14 日	Dan Zetzl	初稿。
01.00	2021 年 11 月 19 日	Dan Zetzl	纳入审查意见后的第一版。
01.01	2022 年 3 月 23 日	Dan Zetzl	更新了表 2 中的 URL，以了解对讲机中心 https 条目和物联网地址中的打字错误。
01.02	2023 年 1 月 25 日		新增了俄语。

表 1：文档修订历史记录

参考资料

[1] 对讲机管理系统规划师，MN004686A01

[2] 禁用 DNS 客户端缓存，
https://docs.microsoft.com/en-us/windows-server/networking/dns/troubleshoot/disable-dns-client-side-caching

简介

MOTOTRBO Ion 和 R7 设备需要先完成一次性激活才能启用随设备购买的软件功能和服务。

为了简化一次性激活并支持没有显示屏的设备，MOTOTRBO 设备随附了默认 Wi-Fi 网络配置文件。除了一次性激活 MOTOTRBO 设备外，使用 Radio Management 或 Radio Central 应用程序的客户还可以选择使用相同的 Wi-Fi 网络，将设备零接触注册到这些应用程序中。

本文档提供针对用于一次性激活的 Wi-Fi 网络在安全性和操作方面的最佳做法建议。

Wi-Fi 网络的最佳做法建议

IP 地址分配

默认情况下，MOTOTRBO 设备会配置为通过 DHCP 获取 IP 地址。提供以下建议是为了确保 DHCP 服务使用的 IP 地址池在设备的批量编程过程中不会耗尽。

1. 我们建议您将 DHCP 服务器配置为使用较短的 DHCP 租用时间。这允许您在完成批量对讲机时重复使用相同的 IP 地址。
2. 我们建议您为 DHCP 服务器配置足够数量的 IP 地址，以便为您在批量配置期间将同时编程的大量 MOTOTRBO 设备以及网络上的其他设备（如对讲机管理设备编程器）提供地址。注：您需要考虑上述 DHCP 租用时间何时到期，以便可以重复使用这些 IP 地址。

MOTOTRBO 设备发现（对讲机管理）

默认情况下，MOTOTRBO 设备被配置为在连接到 Wi-Fi 网络时发送 mDNS-SD[1] 消息，之后每 90 秒发送一次。对讲机管理设备编程器还会发送 mDNS-SD 消息。我们提供的以下建议可以使 Radio Management 软件能够自动发现和读取 MOTOTRBO 设备，而无需用户执行任何操作。

1. DNS-SD 的 UDP 端口号是端口 5353。IPv4 地址是 224.0.0.251。网络防火墙规则必须允许此端口号和广播，服务才能运行。
2. MOTOTRBO 设备和对讲机管理设备编程器必须位于同一网段上，或者必须在网段之间转发多播流量（例如，使用 VLAN[2]）。有关如何配置网络设备以转发多播流量的详细信息，通常可在网络设备制造商的产品资料中找到。

   注：服务发现目标可以使用 Radio Management 软件更新为单播 IP 或主机名。

有关详细信息，请参见对讲机管理系统规划师。

[1] 多播域名服务发现

[2] 虚拟局域网

网络时间服务器可用性

默认情况下，MOTOTRBO 设备会配置为通过 NTP 获取当前时间 [3]。

主要 NTP 服务器	pool.ntp.org
辅助 NTP 服务器	time.google.com

使用 SCEP[4] 注册证书的 MOTOTRBO 设备需要准确的时间作为 CSR[5] 的一部分。要可靠地连接到 Radio Central 云服务，需要准确的时间。

Wi-Fi 信道使用情况

所有 MOTOTRBO 设备均支持 Wi-Fi 第 1 代 (802.11b)、Wi-Fi 第 3 代 (802.11g) 和 Wi-Fi 第 4 代 (802.11n)。

MOTOTRBO Ion 和 MOTOTRBO R7 还支持 Wi-Fi 第 5 代 (802.11ac)，MOTOTRBO Ion 也支持 Wi-Fi 第 6 代 (802.11ax)。

选择非重叠 Wi-Fi 信道是最佳做法，这样可以最大程度提高网络吞吐量。具体而言，此建议适用于覆盖范围重叠的 Wi-Fi 接入点。这就可以避免 Wi-Fi 接入点之间的相邻信道干扰。

在 2.4 GHz 频谱中，我们建议您为覆盖范围重叠的 Wi-Fi 接入点选择信道 1、6 和 11。注：微波炉等其他干扰源可能会影响网络性能。

在 5 GHz 频谱中，有 24 个非重叠信道（即 36、40、44、48、52、56、60、64、100、104、108、112、116、120、124、128、132、136、140、144、149、153、157、161 和 165）。此外，干扰源较少。默认情况下，某些 Wi-Fi 接入点会通过减慢对 2.4 GHz 的响应速度来将设备“引导”到 5 GHz。

在进行批量配置时，您应考虑使用多个接入点来增加可用的总带宽。

[3] Network Time Protocol
[4] Simple Certificate Enrollment Protocol
[5] Certificate Signing Request

最佳安全做法的建议

使用注册网络将不受信任的客户端与公司网络分开是建议的最佳做法。对于 MOTOTRBO 设备，默认情况下会启用初始注册网络。

Wi-Fi 个人网络预共享密钥 (PSK) SSID - MOTOTRBO
密码：Radio Management

限制对注册网络的物理访问

我们建议的最佳做法是将对注册网络 Wi-Fi 覆盖区域的物理访问限制为受信任的个人。

更改默认 Wi-Fi 网络设置

我们建议的最佳做法是将 Wi-Fi 网络和密码更新为默认值以外的其他内容。

企业 Wi-Fi 网络

从安全角度来看，与 Wi-Fi 个人网络相比，使用 Wi-Fi 企业网络有几个优点。这些优点包括：能够在不影响网络上其他设备的情况下禁用单个设备的网络访问，Wi-Fi 接入点和每个设备之间的流量是唯一加密的，并且能够使用标准的证书管理方法更新用于加密的凭据。MOTOTRBO 设备支持 Wi-Fi 个人网络和 Wi-Fi 企业网络。

使用接入控制列表

访问控制列表 (ACL) 可用于将客户端限制为只能访问注册网络以及激活设备所需的服务器和服务。

应用程序或服务	主机名	端口	方向	协议
NTP	pool.ntp.org time.google.com	123	出站	UDP
DHCP	不适用（网络提供）	67 68	出站 入站	UDP
DNS	不适用（网络提供）	53	出站	TCP 和 UDP
证书管理	https://devicecertmgmt-cmf21.motsolpki.com https://devicecertmgmt-cmf21.motsolpki.com	49682 49684	出站	https
Radio Central	locator.radiocentral.motorolasolutions.com	443	出站	https
Radio Central	Api-us.radiocentarl.motorolasolutions.com Api-au.radiocentarl.motorolasolutions.com	443	出站	https
Radio Central	Usp9rmstorage.blob.core.windows.net aup9rmstorage.blob.core.windows.net	443	出站	https
物联网服务	global.azure-devices-provisioning.net	443	出站	https
物联网服务	iotcs-hub-us.azure-devices.net	8883 年	出站 入站	MQTT

表 2：用于一次性激活的设备网络连接

改訂履歴

改訂	日付	作成者	更新の説明
プレリリース	2021 年 11 月 14 日	Dan Zetzl	初回ドラフト。
01.00	2021 年 11 月 19 日	Dan Zetzl	レビュー コメント追加後のリリース 1。
01.01	2022 年 3 月 23 日	Dan Zetzl	表 2 の URL (Radio Central の https エントリの誤字) と IoT アドレスを更新。
01.02	2023 年 1 月 25 日		ロシア語を追加。

表 1: ドキュメントの改訂履歴

参照

[1] Radio Management System Planner、MN004686A01

[2] DNS クライアント側キャッシュを無効にする
https://docs.microsoft.com/en-us/windows-server/networking/dns/troubleshoot/disable-dns-client-side-caching

はじめに

MOTOTRBO Ion および R7 デバイスでは、デバイスと共に購入したソフトウェア機能とサービスを有効にするため、ワンタイム アクティベーションが必要です。

ワンタイム アクティベーションの簡素化と、ディスプレイのないデバイスのサポートのため、MOTOTRBO デバイスにはデフォルトの Wi-Fi ネットワーク プロファイルが付属しています。MOTOTRBO デバイスのワンタイム アクティベーションに加えて、Radio Management アプリケーションまたは Radio Central アプリケーションを使用しているお客様は、これらのアプリケーションにデバイスをゼロタッチで登録するために、同じ Wi-Fi ネットワークを使用することを選択できます。

このドキュメントでは、ワンタイム アクティベーションに使用する Wi-Fi ネットワークのセキュリティと運用に関するベスト プラクティスの推奨事項について説明します。

Wi-Fi ネットワークのベスト プラクティスに関する推奨事項

IP アドレスの割り当て

MOTOTRBO デバイスは、DHCP 経由で IP アドレスを取得するようにデフォルトで設定されています。以下は、デバイスの一括プログラミング中に DHCP サービスが使用する IP アドレスのプールが空にならないようにするための推奨事項です。

1. DHCP サーバーは、短い DHCP リース時間を使用するように設定することをお勧めします。これにより、同じ構成を共有する無線機が完了したときに同じ IP アドレスを再利用できます。
2. 一括プロビジョニング中に同時にプログラムする MOTOTRBO デバイスと、Radio Management Device Programmer などのネットワーク上にある他のデバイスにアドレスを提供するため、DHCP サーバーに十分な数の IP アドレスを設定することをお勧めします。注意: これらの IP アドレスを再利用するため、先述の DHCP リースの有効期限を考慮しておく必要があります。

MOTOTRBO デバイス検出 (Radio Management)

MOTOTRBO デバイスは、Wi-Fi ネットワークへの接続時およびその後 90 秒ごとに、mDNS-SD[1] メッセージを送信するようにデフォルトで設定されています。また、Radio Management Device Programmer も mDNS-SD メッセージを送信します。以下は、Radio Management ソフトウェアを有効にし、ユーザーの操作なしに MOTOTRBO デバイスを自動的に検出して読み取るための推奨事項です。

1. DNS-SD の UDP ポート番号はポート 5353 です。IPv4 アドレスは 224.0.0.251 です。ネットワーク ファイアウォールのルールでは、このポート番号とブロードキャストを許可して、サービスを動作させる必要があります。
2. MOTOTRBO デバイスと Radio Management Device Programmer は、同じネットワークセグメント上にある必要があります。そうでない場合は、マルチキャスト トラフィックをネットワークセグメント間 (たとえば、VLAN[2] を使用) で転送する必要があります。マルチキャスト トラフィックを転送するようにネットワーク機器を設定する方法の詳細については、ネットワーク機器メーカーの製品資料を参照してください。

[1]マルチキャスト ドメイン ネーム サービス サービス ディスカバリ
[2]仮想ローカル エリア ネットワーク

注: サービス ディスカバリの宛先は、Radio Management ソフトウェアを使用してユニキャスト IP またはホスト名に更新できます。

詳細については、『Radio Management System Planner』を参照してください。

ネットワーク タイム サーバーの利用可否

MOTOTRBO デバイスは、デフォルトで、NTP[3] を介して現在の時刻を取得するように設定されています。

プライマリ NTP サーバー	pool.ntp.org
セカンダリ NTP サーバー	time.google.com

SCEP[4] を使用して証明書を登録する MOTOTRBO デバイスでは、CSR[5] の一部として正確な時刻が必要となります。Radio Central クラウドサービスに高い信頼性で接続するには、正確な時刻が必要となります。

Wi-Fi チャネルの使用

すべての MOTOTRBO デバイスは、Wi-Fi 第 1 世代 (802.11b)、Wi-Fi 第 3 世代 (802.11g)、および Wi-Fi 第 4 世代 (802.11n) をサポートしています。

MOTOTRBO Ion および MOTOTRBO R7 は、Wi-Fi 第 5 世代 (802.11ac) もサポートしており、MOTOTRBO Ion は Wi-Fi 第 6 世代 (802.11ax) もサポートしています。

ネットワークのスループットを最大化するには、重複していない Wi-Fi チャンネルを選択することをお勧めします。特に、この推奨事項は通信範囲が重複している Wi-Fi アクセス ポイントに適用されます。これにより、Wi-Fi アクセス ポイント間の隣接チャネル干渉を回避できます。

[3] Network Time Protocol
[4] Simple Certificate Enrollment Protocol
[5] Certificate Signing Request

2.4GHz スペクトルでは、重複する通信範囲がある Wi-Fi アクセス ポイントには、チャネル 1、6 および 11 を選択することをお勧めします。注意: 電子レンジなどの他の干渉源が、ネットワークのパフォーマンスに干渉する可能性があります。

5GHz スペクトルには、24 の非重複チャネル (36、40、44、48、52、56、60、64、100、104、108、112、116、120、124、128、132、136、140、144、149、153、157、161、165) があります。また、干渉源も少なくなります。デフォルトでは、一部の Wi-Fi アクセス ポイントは 2.4GHz への応答を遅くすることで、5 GHz にデバイスを「誘導」します。

一括プロビジョニング時には、複数のアクセス ポイントを使用して利用可能な総帯域幅を増やすことを検討する必要があります。

セキュリティのベスト プラクティスに関する推奨事項

登録ネットワークを使用して、信頼できないクライアントを企業ネットワークから分離することが、推奨されるベスト プラクティスです。MOTOTRBO デバイスの場合、初期登録ネットワークがデフォルトで有効になっています。

Wi-Fi パーソナル ネットワーク事前共有キー (PSK) SSID - MOTOTRBO
パスフレーズ: Radio Management

登録ネットワークへの物理アクセスを制限する

登録ネットワークの Wi-Fi 通信範囲への物理アクセスを信頼できる個人に制限することが、推奨されるベスト プラクティスです。

デフォルトの Wi-Fi ネットワーク設定を変更する

Wi-Fi ネットワークとパスフレーズをデフォルトの値から変更することが、推奨されるベスト プラクティスです。

エンタープライズ Wi-Fi ネットワーク

セキュリティの観点では、パーソナル Wi-Fi ネットワークよりもエンタープライズ Wi-Fi ネットワークを使用したほうが得られるメリットは多いです。具体的には、ネットワーク上の他のデバイスに影響を与えることなく、個々のデバイス単位でネットワーク アクセスを無効にできること、Wi-Fi アクセス ポイントと各デバイス間でトラフィックを一意に暗号化できること、標準的な証明書管理方法を使用して、暗号化に使用される資格情報を更新できることなどがあります。MOTOTRBO デバイスは、パーソナル Wi-Fi ネットワークとエンタープライズ Wi-Fi ネットワークの両方をサポートしています。

アクセス コントロール リストを使用する

アクセス コントロール リスト (ACL) を使用して、クライアントを登録ネットワークとデバイスのアクティベーションに必要なサーバーとサービスのみに制限できます。

アプリケーションまたはサービス	ホスト名	ポート	方向	プロトコル
NTP	Pool.ntp.org time.google.com	123	アウトバウンド	UDP
DHCP	N/A (ネットワーク指定)	67 68	アウトバウンド インバウンド	UDP
DNS	N/A (ネットワーク指定)	53	アウトバウンド	TCP および UDP
証明書管理	https://devicecertmgmt-cmf21.motsolpki.com https://devicecertmgmt-cmf21.motsolpki.com	49682 49684	アウトバウンド	https
Radio Central	locator.radiocentral.motorolasolutions.com	443	アウトバウンド	https
Radio Central	Api-us.radiocentral.motorolasolutions.com Api-au.radiocentral.motorolasolutions.com	443	アウトバウンド	https

アプリケーションまたはサービス	ホスト名	ポート	方向	プロトコル
Radio Central	Usp9rmstorage.blob.core.windows.net aup9rmstorage.blob.core.windows.net	443	アウトバウンド	https
IoT サービス	global.azure-devices-provisioning.net	443	アウトバウンド	https
IoT サービス	iotcs-hub-us.azure-devices.net	8883	アウトバウンド インバウンド	MQTT

表 2: ワンタイム アクティベーションのためのデバイス ネットワーク接続

개정 기록

개정	날짜	작성자	업데이트 설명
사전 릴리스	2021/11/14	Dan Zetzl	최초 초안.
01.00	2021/11/19	Dan Zetzl	통합 의견 검토 후 릴리스.
01.01	2022/03/23	Dan Zetzl	표 2 URL 의 Radio Central https 입력 및 IoT 주소 오타 업데이트.
01.02 년	2023/1/25		러시아어가 추가되었습니다.

표 1: 문서 개정 기록

참조

[1] Radio Management 시스템 플래너, MN004686A01

[2] DNS 클라이언트 측 캐싱 비활성화, https://docs.microsoft.com/en-us/windows-server/networking/dns/troubleshoot/disable-dns-client-side-caching

소개

MOTOTRBO Ion 및 R7 장치는 장치와 함께 구매한 소프트웨어 기능과 서비스를 사용하려면 일회성 활성화를 거쳐야 합니다.

일회성 활성화를 간소화하고 디스플레이가 없는 장치를 지원하기 위해 MOTOTRBO 장치는 기본 Wi-Fi 네트워크 프로필과 함께 제공됩니다. MOTOTRBO 장치를 1 회 활성화하는 것 외에도, Radio Management 또는 Radio Central 애플리케이션을 사용하는 고객은 동일한 Wi-Fi 네트워크를 이용하여 장치를 해당 애플리케이션에 제로 터치 등록하도록 선택할 수 있습니다.

본 문서는 일회성 활성화에 사용되는 Wi-Fi 네트워크의 보안 및 작동과 관련된 권장 모범 사례를 제공합니다.

Wi-Fi 네트워크 권장 모범 사례

IP 주소 할당

MOTOTRBO 장치는 기본적으로 DHCP 를 통해 IP 주소를 획득하도록 구성됩니다. 장치의 일괄 프로그래밍 중에 DHCP 서비스에서 사용하는 IP 주소 풀이 소모되지 않도록 하려면 다음 권장 사항을 참조하십시오.

1. 짧은 DHCP 임대 시간을 사용하도록 DHCP 서버를 구성하는 것이 좋습니다. 이렇게 하면 무전기를 일괄 완료할 때와 동일한 IP 주소를 재사용할 수 있습니다.
2. 일괄 프로비저닝 중에 동시에 프로그래밍할 여러 MOTOTRBO 장치 및 Radio Management 장치 프로그래머와 같은 네트워크에 있는 다른 장치에 주소를 제공할 수 있도록 DHCP 서버를 충분한 양의 IP 주소로 구성하는 것이 좋습니다. 참고: 앞서 설명한 DHCP 임대가 만료되는 시점을 고려해야 IP 주소를 재사용할 수 있습니다.

MOTOTRBO 장치 검색(Radio Management)

기본적으로 MOTOTRBO 장치는 Wi-Fi 네트워크에 연결할 때와 이후 90 초마다 mDNS-SD[1] 메시지를 전송하도록 구성됩니다. Radio Management 장치 프로그래머는 mDNS-SD 메시지도 전송합니다. 사용자가 별다른 작업을 수행하지 않고도 Radio Management 소프트웨어가 MOTOTRBO 장치를 자동으로 검색하고 읽어들일 수 있도록 하려면 다음 권장 사항을 참조하십시오.

1. DNS-SD 의 UDP 포트 번호는 포트 5353 입니다. IPv4 주소는 224.0.0.251 입니다. 네트워크 방화벽 규칙에서 이 포트 번호와 브로드캐스트를 허용해야 서비스가 작동합니다.
2. MOTOTRBO 장치와 Radio Management 장치 프로그래머는 동일한 네트워크 세그먼트에 있거나 멀티캐스트 트래픽을 네트워크 세그먼트 간에 전달해야 합니다(예: VLAN[2] 사용). 멀티캐스트 트래픽을 전달하도록 네트워크 장비를 구성하는 방법에 대한 세부 내용은 일반적으로 네트워크 장비 제조업체의 제품 설명서에서 확인할 수 있습니다.

[1] 멀티캐스트 도메인 이름 서비스 서비스 검색
[2] 가상 로컬 영역 네트워크

참고: 서비스 검색 대상은 Radio Management 소프트웨어를 사용하여 유니캐스트 IP 또는 호스트 이름으로 업데이트할 수 있습니다.

자세한 내용은 Radio Management 시스템 플래너를 참조하십시오.

네트워크 시간 서버 가용성

MOTOTRBO 장치는 기본적으로 NTP[3]를 통해 현재 시간을 알 수 있도록 구성됩니다.

기본 NTP 서버	pool.ntp.org
보조 NTP 서버	time.google.com

SCEP[4]를 사용하여 인증서를 등록하는 MOTOTRBO 장치는 CSR[5]의 일부로서 정확한 시간이 필요합니다. Radio Central 클라우드 서비스에 안정적으로 연결하려면 정확한 시간이 필요합니다.

Wi-Fi 채널 사용

모든 MOTOTRBO 장치는 Wi-Fi 1 세대(802.11b), Wi-Fi 3 세대(802.11g) 및 Wi-Fi 4 세대(802.11n)를 지원합니다.

MOTOTRBO Ion 및 MOTOTRBO R7 은 Wi-Fi 5 세대(802.11ac)도 지원하며, MOTOTRBO Ion 은 Wi-Fi 6 세대(802.11ax)를 추가로 지원합니다.

네트워크에서 처리량을 극대화하려면 겹치지 않는 Wi-Fi 채널을 선택하는 것이 좋습니다. 특히 이 권장 사항은 통신 범위가 중복되는 Wi-Fi 액세스 포인트에 해당합니다. 이렇게 하면 Wi-Fi 액세스 포인트 사이의 인접 채널 간섭을 방지할 수 있습니다.

[3] Network Time Protocol
[4] Simple Certificate Enrollment Protocol
[5] Certificate Signing Request

2.4GHz 스펙트럼에서는 통신 범위가 겹치는 Wi-Fi 액세스 포인트로 채널 1, 6, 11 을 선택하는 것이 좋습니다. 참고: 전자레인지와 같은 다른 간섭원은 네트워크 성능을 저해할 수 있습니다.

5GHz 스펙트럼에는 24 개의 비중복 채널(36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161, 165)이 있습니다. 게다가 간섭원도 더 적습니다. 기본적으로 일부 Wi-Fi 액세스 포인트는 2.4GHz 에 대한 응답을 지연시켜 장치를 5GHz 로 '전환'합니다.

일괄 프로비저닝 시 사용 가능한 총 대역폭을 늘리려면 여러 액세스 포인트를 사용해야 합니다.

보안 권장 모범 사례

등록 네트워크를 사용하여 신뢰할 수 없는 클라이언트를 회사 네트워크에서 분리하는 것이 좋습니다. MOTOTRBO 장치의 경우 초기 등록 네트워크가 기본적으로 활성화됩니다.

Wi-Fi 개인용 네트워크 사전 공유 키(PSK) SSID - MOTOTRBO
암호구: Radio Management

등록 네트워크에 대한 물리적 액세스 제한

신뢰할 수 있는 개인만 등록 네트워크의 Wi-Fi 범위 영역에 물리적으로 액세스할 수 있도록 제한하는 것이 좋습니다.

기본 Wi-Fi 네트워크 설정 변경

Wi-Fi 네트워크 및 암호구를 기본값이 아닌 다른 값으로 업데이트하는 것이 좋습니다.

기업용 Wi-Fi 네트워크

기업용 Wi-Fi 네트워크를 사용하면 개인용 Wi-Fi 네트워크를 사용할 때와 비교해서 몇 가지 보안상 이점이 있습니다. 네트워크의 다른 장치에 영향을 주지 않고 개별 장치를 기준으로 네트워크 액세스를 비활성화할 수 있는 기능, Wi-Fi 액세스 포인트와 각 장치 간에 고유하게 암호화되는 트래픽, 표준 인증서 관리를 통해 암호화에 사용되는 자격 증명을 업데이트할 수 있는 기능 등이 이러한 장점에 해당합니다. MOTOTRBO 장치는 개인용 Wi-Fi 및 기업용 Wi-Fi 네트워크를 모두 지원합니다.

액세스 제어 목록 사용

액세스 제어 목록(ACL)을 사용하여 등록 네트워크와 장치 활성화에 필요한 서버 및 서비스만으로 클라이언트를 제한할 수 있습니다.

애플리케이션 또는 서비스	호스트 이름	포트	방향	프로토콜
NTP	Pool.ntp.org time.google.com	123	아웃바운드	UDP
DHCP	해당 없음(네트워크 제공됨)	67 68	아웃바운드 인바운드	UDP
DNS	해당 없음(네트워크 제공됨)	53	아웃바운드	TCP 및 UDP
인증서 관리	https://devicecertmgmt-cmf21.motsolpki.com https://devicecertmgmt-cmf21.motsolpki.com	49682 49684	아웃바운드	https
Radio Central	locator.radiocentral.motorolasolutions.com	443	아웃바운드	https
Radio Central	Api-us.radiocentral.motorolasolutions.com Api-au.radiocentral.motorolasolutions.com	443	아웃바운드	https
Radio Central	Usp9rmstorage.blob.core.windows.net aup9rmstorage.blob.core.windows.net	443	아웃바운드	https
IoT 서비스	global.azure-devices-provisioning.net	443	아웃바운드	https
IoT 서비스	iotcs-hub-us.azure-devices.net	8883	아웃바운드 인바운드	MQTT

표 2: 일회성 활성화를 위한 장치 네트워크 연결

Riwayat Revisi

Revisi	Tanggal	Penyusun	Deskripsi Pembaruan
Pra-Rilis	14/11/2021	Dan Zetzl	Draf Awal.
01.00	19/11/2021	Dan Zetzl	Rilis satu setelah memasukkan komentar tinjauan.
01.01	23/3/2022	Dan Zetzl	Pembaruan URL dalam Tabel 2 karena kesalahan ketik pada entri https Radio Central dan alamat IoT.
01.02	25/1/2023		Penambahan Bahasa Rusia.

Tabel 1: Riwayat Revisi Dokumen

Referensi

[1] Perencana Sistem Radio Management, MN004686A01

[2] Menonaktifkan Penyimpanan Cache dari Sisi Klien DNS, https://docs.microsoft.com/en-us/windows-server/networking/dns/troubleshoot/disable-dns-client-side-caching

Pengantar

Perangkat MOTOTRBO Ion dan R7 memerlukan aktivasi satu kali untuk mengaktifkan fitur dan layanan perangkat lunak yang telah dibeli bersama perangkat.

Untuk menyederhanakan aktivasi satu kali dan untuk mendukung perangkat tanpa layar, perangkat MOTOTRBO dikirim dengan profil jaringan Wi-Fi default. Selain aktivasi satu kali pada perangkat MOTOTRBO, pelanggan yang menggunakan aplikasi Radio Management atau Radio Central dapat memilih untuk menggunakan jaringan Wi-Fi yang sama untuk pendaftaran tanpa sentuhan pada perangkat ke aplikasi tersebut.

Dokumen ini memberikan rekomendasi praktik terbaik terkait keamanan dan pengoperasian jaringan Wi-Fi yang digunakan untuk aktivasi satu kali.

Rekomendasi Praktik Terbaik untuk Jaringan Wi-Fi

Penetapan Alamat IP

Perangkat MOTOTRBO dikonfigurasi, secara default, untuk mendapatkan alamat IP melalui DHCP. Rekomendasi berikut disediakan guna memastikan pool alamat IP yang digunakan oleh layanan DHCP tidak habis selama pemrograman perangkat secara massal.

1. Anda dianjurkan untuk mengonfigurasi server DHCP untuk menggunakan waktu sewa DHCP yang singkat. Ini memungkinkan Anda menggunakan kembali alamat IP yang sama setelah beberapa batch radio selesai.
2. Anda dianjurkan untuk mengonfigurasi server DHCP dengan jumlah alamat IP yang memadai untuk menyediakan alamat ke jumlah perangkat MOTOTRBO yang akan Anda program secara bersamaan selama penyiapan massal ditambah perangkat lain yang akan ada di jaringan seperti Pemrogram Perangkat Radio Management. Catatan: Anda perlu mempertimbangkan kapan sewa DHCP, seperti dijelaskan di atas, akan berakhir sehingga Anda dapat menggunakan kembali alamat IP tersebut.

Penemuan Perangkat MOTOTRBO (Radio Management)

Perangkat MOTOTRBO dikonfigurasi, secara default, untuk mengirim pesan mDNS-SD[1] saat menghubungkan ke jaringan Wi-Fi dan setiap 90 detik setelahnya. Pemrogram Perangkat Radio Management juga mengirim pesan mDNS-SD. Rekomendasi berikut disediakan agar perangkat lunak Radio Management dapat menemukan dan membaca perangkat MOTOTRBO secara otomatis tanpa pengguna perlu melakukan tindakan apa pun.

1. Nomor port UDP untuk DNS-SD adalah port 5353. Alamat IPv4 adalah 224.0.0.251. Aturan firewall jaringan harus mengizinkan nomor port ini dan disiarkan agar layanan dapat beroperasi.
2. Perangkat MOTOTRBO dan Pemrogram Perangkat Radio Management harus berada pada segmen jaringan yang sama atau lalu lintas multicast harus diteruskan antara segmen jaringan (misalnya, menggunakan VLAN[2]). Perincian mengenai cara mengonfigurasi peralatan jaringan untuk meneruskan lalu lintas multicast biasanya dapat ditemukan dalam publikasi produk produsen peralatan jaringan Anda.

[1] Penemuan Layanan Multicast Domain Name Service
[2] Jaringan Area Lokal Virtual

Catatan: Tujuan penemuan layanan dapat diperbarui ke IP unicast atau nama host menggunakan perangkat lunak Radio Management.

Harap baca Perencana Sistem Radio Management untuk mendapatkan informasi lebih lanjut.

Ketersediaan Server Waktu Jaringan

Secara default, perangkat MOTOTRBO dikonfigurasikan untuk mendapatkan waktu saat ini melalui NTP[3].

Server NTP Utama	pool.ntp.org
Server NTP Sekunder	time.google.com

Perangkat MOTOTRBO yang mendaftar untuk sertifikat menggunakan SCEP[4] memerlukan waktu yang akurat sebagai bagian dari CSR[5]. Waktu yang akurat diperlukan untuk koneksi yang andal dengan layanan cloud Radio Central.

Penggunaan Saluran Wi-Fi

Semua perangkat MOTOTRBO mendukung Wi-Fi Generasi 1 (802.11b), Wi-Fi Generasi 3 (802.11g), dan Wi-Fi Generasi 4 (802.11n).

MOTOTRBO Ion dan MOTOTRBO R7 juga mendukung Wi-Fi Generasi 5 (802.11ac) dan MOTOTRBO Ion juga mendukung Wi-Fi Generasi 6 (802.11ax).

Memilih saluran Wi-Fi yang tidak tumpang tindih untuk memaksimalkan throughput pada jaringan adalah praktik terbaik. Secara khusus, rekomendasi ini berlaku untuk titik akses Wi-Fi dengan jangkauan yang tumpang tindih. Ini guna menghindari interferensi saluran yang berdekatan di antara titik akses Wi-Fi.

[3] Network Time Protocol
[4] Simple Certificate Enrollment Protocol
[5] Certificate Signing Request

Pada spektrum 2,4 GHz, Anda disarankan untuk memilih saluran 1, 6, dan 11 untuk titik akses Wi-Fi dengan jangkauan yang tumpang tindih. Catatan: Sumber interferensi lain seperti oven microwave dapat mengganggu kinerja jaringan.

Pada spektrum 5 GHz, terdapat 24 saluran yang tidak tumpang tindih (36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161, dan 165). Selain itu, sumber interferensi lebih sedikit. Secara default, beberapa titik akses Wi-Fi akan "mengarahkan" perangkat ke 5 GHz dengan memperlambat respons ke 2,4 GHz.

Penggunaan beberapa titik akses untuk meningkatkan total bandwidth yang tersedia harus dipertimbangkan saat penyediaan massal.

Rekomendasi Praktik Terbaik untuk Keamanan

Penggunaan jaringan pendaftaran untuk memisahkan klien tidak tepercaya dari jaringan korporat merupakan praktik terbaik yang disarankan. Pada kasus perangkat MOTOTRBO, jaringan pendaftaran awal diaktifkan secara default.

SSID Pre-Shared Key (PSK) Jaringan Pribadi Wi-Fi - MOTOTRBO
Frasa Sandi: Radio Management

Membatasi Akses Fisik ke Jaringan Pendaftaran

Praktik terbaik yang disarankan adalah membatasi akses fisik ke area jangkauan Wi-Fi jaringan pendaftaran kepada orang-orang yang dipercaya.

Mengubah Pengaturan Jaringan Wi-Fi Default

Praktik terbaik yang disarankan adalah memperbarui jaringan Wi-Fi dan frasa sandi dengan nilai selain nilai default.

Jaringan Wi-Fi Enterprise

Dari sudut pandang keamanan, penggunaan jaringan Wi-Fi Enterprise memberikan beberapa keuntungan jika dibandingkan dengan jaringan Wi-Fi pribadi. Keuntungan tersebut meliputi kemampuan untuk menonaktifkan akses jaringan di setiap perangkat tanpa memengaruhi perangkat lain di jaringan, lalu lintas dienkripsi secara unik di antara titik akses Wi-Fi dan setiap perangkat, serta kemampuan untuk memperbarui kredensial yang digunakan untuk enkripsi menggunakan praktik manajemen sertifikat standar. Perangkat MOTOTRBO mendukung jaringan Wi-Fi Pribadi dan Wi-Fi Enterprise.

Menggunakan Access Control List

Access Control List (ACL) dapat digunakan untuk membatasi klien hanya ke jaringan pendaftaran dan server serta layanan yang diperlukan untuk mengaktifkan perangkat.

Aplikasi atau Layanan	Nama Host	Port	Arah	Protokol
Network Time Protocol/NTP	Pool.ntp.org time.google.com	123	Keluar	User Datagram Protocol/UDP
Dynamic Host Configuration Protocol/DHCP	tidak ada (jaringan disediakan)	67 68	Keluar Masuk	User Datagram Protocol/UDP
Domain Name System/DNS	tidak ada (jaringan disediakan)	53	Keluar	TCP & UDP
Certificate Management	https://devicecertmgmt-cmf21.motsolpki.com https://devicecertmgmt-cmf21.motsolpki.com	49682 49684	Keluar	https
Radio Central	locator.radiocentral.motorolasolutions.com	443	Keluar	https
Radio Central	Api-us.radiocentral.motorolasolutions.com Api-au.radiocentral.motorolasolutions.com	443	Keluar	https
Radio Central	Usp9rmstorage.blob.core.windows.net aup9rmstorage.blob.core.windows.net	443	Keluar	https
Layanan IoT	global.azure-devices-provisioning.net	443	Keluar	https
Layanan IoT	iotcs-hub-us.azure-devices.net	8883	Keluar Masuk	MQTT

Tabel 2: Koneksi Jaringan Perangkat untuk Aktivasi Satu Kali

Versionsverlauf

Revision	Datum	Autor	Beschreibung der Aktualisierungen
Vorab-Training	14.11.2021	Dan Zetzl	Erster Entwurf.
01,00	19.11.2021	Dan Zetzl	Version 1 nach der Aufnahme der Kommentare aus der Überprüfung.
01,01	23.03.2022	Dan Zetzl	URLs in Tabelle 2 wegen eines Tippfehlers im Radio Central-HTTPS-Eintrag und der IoT-Adresse aktualisiert.
01,02	25.01.2023		Russische Sprache hinzugefügt.

Tabelle 1: Verlauf der Dokumentrevision

Referenzen

[1] Funkgerätverwaltungssystem-Planer, MN004686A01

[2] Clientseitiges DNS-Caching deaktivieren, https://docs.microsoft.com/en-us/windows-server/networking/dns/troubleshoot/disable-dns-client-side-caching

Einführung

Das MOTOTRBO ION- und R7-Gerät erfordern eine einmaligen Aktivierung der Softwarefunktionen und Dienste, die mit dem Gerät erworben wurden.

Um die einmalige Aktivierung zu vereinfachen und Geräte ohne Display zu unterstützen, werden die MOTOTRBO-Geräte mit einem standardmäßigen WLAN-Netzwerkprofil ausgeliefert. Zusätzlich zur einmaligen Aktivierung der MOTOTRBO-Geräte können Kunden, die die Anwendung „Radio Management“ oder „Radio Central“ verwenden, dasselbe WLAN-Netzwerk zur Zero-Touch-Registrierung des Geräts in diesen Anwendungen nutzen.

Dieses Dokument enthält Best-Practice-Empfehlungen für die Sicherheit und den Betrieb des WLAN-Netzwerks, das zur einmaligen Aktivierung verwendet wird.

Best-Practice-Empfehlungen für das WLAN-Netzwerk

Zuordnung von IP-Adressen

MOTOTRBO-Geräte sind standardmäßig dazu konfiguriert, eine IP-Adresse über DHCP erhalten. Die folgenden Empfehlungen werden bereitgestellt, um zu gewährleisten, dass der vom DHCP-Dienst verwendete Pool von IP-Adressen während der Massenprogrammierung von Geräten nicht vollständig aufgebraucht wird.

1. Es wird empfohlen, den DHCP-Server zur Nutzung kurzer DHCP-Lease-Zeiten zu konfigurieren. Auf diese Weise können Sie dieselben IP-Adressen wiederverwenden, wenn mehrere Funkgeräte fertiggestellt werden.
2. Es wird empfohlen, Ihren DHCP-Server mit einer ausreichenden Anzahl von IP-Adressen zu konfigurieren, um Adressen für die während der Massenbereitstellung gleichzeitig programmierten Anzahl an MOTOTRBO-Geräten sowie für die anderen im Netzwerk befindlichen Geräte, z. B. den Radio Management-Geräteprogrammierer, bereitzustellen. Hinweis: Sie müssen beachten, wann der oben beschriebene DHCP-Lease abläuft, damit Sie diese IP-Adressen wiederverwenden können.

MOTOTRBO Device Discovery (Radio Management)

MOTOTRBO-Geräte sind standardmäßig dazu konfiguriert, wenn sie sich mit einem WLAN-Netzwerk verbinden und danach alle 90 Sekunden, eine mDNS-SD[1]-Nachricht zu senden. Der Radio Management-Geräteprogrammierer sendet ebenfalls mDNS-SD-Nachrichten. Die folgenden Empfehlungen dienen dazu, der Radio Management-Software zu ermöglichen, MOTOTRBO-Geräte automatisch zu erkennen und zu lesen, ohne dass eine Aktion des Benutzers nötig wäre.

1. Die UDP-Portnummer von DNS-SD ist Port 5353. Die IPv4-Adresse lautet 224.0.0.251. Die Regeln der Netzwerk-Firewall müssen diese Portnummer und die Übertragung zulassen, damit der Dienst ausgeführt werden kann.
2. Das MOTOTRBO-Gerät und der Radio Management-Geräteprogrammierer müssen sich im selben Netzwerksegment befinden oder der Multicast-Verkehr muss zwischen den Netzwerksegmenten weitergeleitet werden (z. B. per VLAN[2]). Einzelheiten zur Konfiguration Ihrer Netzwerkgeräte zur Weiterleitung von Multicast-Verkehr finden Sie in der Produktliteratur des Netzwerkgeräteherstellers.

[1] Ermittlung des Multicast Domain Name Service
[2] Virtuelles lokales Netzwerk

Hinweis: Das Ziel der Service-Ermittlung kann mithilfe der Radio Management-Software zu einer Unicast-IP oder einem Hostnamen aktualisiert werden.

Weitere Informationen finden Sie im Funkgerätverwaltungssystem-Planer.

Verfügbarkeit des Network Time Servers

MOTOTRBO-Geräte sind standardmäßig dazu konfiguriert, die aktuelle Uhrzeit über den NTP[3] abzurufen.

Primärer NTP-Server	pool.ntp.org
Sekundärer NTP-Server	time.google.com

MOTOTRBO-Geräte, die sich für Zertifikate mit SCEP[4] registrieren, benötigen eine genaue Zeit als Teil der CSR[5]. Eine zuverlässige Verbindung mit dem Radio Central Cloud-Service erfordert eine genaue Zeit.

Nutzung von WLAN-Kanälen

Alle MOTOTRBO-Geräte unterstützen WLAN-Generation 1 (802.11b), WLAN-Generation 3 (802.11g) und WLAN-Generation 4 (802.11n).

Das MOTOTRBO Ion und das MOTOTRBO R7 unterstützen ebenfalls WLAN-Generation 5 (802.11ac) und das MOTOTRBO Ion unterstützt außerdem WLAN-Generation 6 (802.11ax).

Es ist Best Practice, keine überlappenden WLAN-Kanäle auszuwählen, um den Netzwerkdurchsatz zu maximieren. Diese Empfehlung gilt insbesondere für WLAN-Zugriffspunkte mit überlappender Abdeckung. Dies verhindert eine Nachbarkanalinterferenz zwischen den WLAN-Zugriffspunkten.

[3] Network Time Protocol
[4] Simple Certificate Enrollment Protocol
[5] Certificate Signing Request

Im 2,4-GHz-Spektrum wird empfohlen bei WLAN-Zugriffspunkten mit sich überlappender Abdeckung die Kanäle 1, 6 und 11 auszuwählen. Hinweis: Andere Störquellen wie Mikrowellengeräte können die Netzwerkleistung beeinträchtigen.

Im 5-GHz-Spektrum gibt es 24 Kanäle, sie sich nicht überlappen (36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161 und 165). Außerdem gibt es dort weniger Störquellen. Standardmäßig „steuern“ einige WLAN-Zugriffspunkte Geräte zum 5-GHz-Spektrum, indem sie Antworten auf 2,4 GHz verlangsamen.

Bei der Massenbereitstellung sollte erwogen werden, mehrere Zugriffspunkte zu verwenden, um die gesamte verfügbaren Bandbreite zu erhöhen.

Best-Practice-Empfehlungen für die Sicherheit

Die Verwendung eines Registrierungsnetzwerks zur Trennung nicht vertrauenswürdiger Clients vom Unternehmensnetzwerk zählt zu den empfohlenen Best Practices. Bei MOTOTRBO-Geräten ist das Netzwerk für die Erstregistrierung standardmäßig aktiviert.

Pre-Shared Key (PSK) für nicht öffentliche WLAN-Netzwerke SSID – MOTOTRBO Passphrase: Radio Management

Beschränken Sie den physischen Zugriff auf das Registrierungsnetzwerk

Es wird empfohlen, den physischen Zugriff auf den WLAN-Abdeckungsbereich des Registrierungsnetzwerks auf vertrauenswürdige Personen zu beschränken.

Ändern Sie die Standard-WLAN-Netzwerkeinstellungen

Es zählt zu den empfohlenen Best Practices, das WLAN-Netzwerk und die Passphrase auf einen anderen Wert als den Standardwert zu aktualisieren.

Unternehmenseigene WLAN-Netzwerke

Vom Sicherheitsstandpunkt aus bietet die Verwendung von unternehmenseigenen WLAN-Netzwerken im Vergleich zu persönlichen WLAN-Netzwerken mehrere Vorteile. Zu den Vorteilen gehört die Möglichkeit, den Netzwerkzugriff auf einzelner Geräte zu deaktivieren, ohne die anderen Geräte im Netzwerk zu beeinträchtigen, dass der Datenverkehr zwischen dem WLAN-Zugriffspunkt und jedem Gerät eindeutig verschlüsselt wird und die Möglichkeit, die für die Verschlüsselung verwendeten Anmeldeinformationen mithilfe von standardmäßigen Zertifikatverwaltungsverfahren zu aktualisieren. MOTOTRBO-Geräte unterstützen sowohl persönliche als auch unternehmenseigene WLAN-Netzwerke.

Verwenden Sie eine Zugriffskontrollliste

Eine Zugriffskontrollliste (ACL) kann verwendet werden, um Clients auf das Registrierungsnetzwerk und die zur Aktivierung des Geräts erforderlichen Server und Services zu beschränken.

Anwendung oder Service	Hostname	Anschluss	Richtung	Protokoll
NTP	Pool.ntp.org time.google.com	123	Ausgehend	UDP
DHCP	k.a. (Netzwerk bereitgestellt)	67 68	Ausgehend Eingehend	UDP
DNS	k.a. (Netzwerk bereitgestellt)	53	Ausgehend	TCP und UDP
Zertifikatsmanagement	https://devicecertmgmt-cmf21.motsolpki.com https://devicecertmgmt-cmf21.motsolpki.com	49682 49684	Ausgehend	HTTPS
RadioCentral	locator.radiocentral.motorolasolutions.com	443	Ausgehend	HTTPS
RadioCentral	Api-us.radiocentral.motorolasolutions.com Api-au.radiocentral.motorolasolutions.com	443	Ausgehend	HTTPS
RadioCentral	Usp9rmstorage.blob.core.windows.net aup9rmstorage.blob.core.windows.net	443	Ausgehend	HTTPS
IoT-Service	global.azure-devices-provisioning.net	443	Ausgehend	HTTPS

Anwendung oder Service	Hostname	Anschluss	Richtung	Protokoll
IoT-Service	iotcs-hub-us.azure-devices.net	8883	Ausgehend Eingehend	MQTT

Tabelle 2: Geräte-Netzwerkverbindungen für die einmalige Aktivierung

Historial de revisiones

Revisión	Fecha	Autor	Descripción de las actualizaciones
Versión preliminar	14/11/21	Dan Zetzl	Borrador inicial.
01.00	19/11/21	Dan Zetzl	Versión uno después de que se incorporaran los comentarios de la revisión.
01.01	23/03/22	Dan Zetzl	Se han actualizado las URL de Tabla 2 por un error en la entrada https de Radio Central y la dirección de IoT.
01.02	25/01/23		Se ha añadido el idioma ruso.

Tabla 1: Historial de revisiones del documento

Referencias

[1] Radio Management System Planner, MN004686A01

[2] Deshabilitar el almacenamiento en caché del lado cliente DNS, https://docs.microsoft.com/en-us/windows-server/networking/dns/troubleshoot/disable-dns-client-side-caching

Introducción

Los dispositivos MOTOTRBO Ion y R7 requieren un proceso de activación de los servicios y las funciones de software adquiridos con el dispositivo.

Para simplificar el proceso de activación y ser compatible con dispositivos sin pantalla, los dispositivos MOTOTRBO se suministran con un perfil de red Wi-Fi predeterminado. Además del proceso de activación de los dispositivos MOTOTRBO, los clientes que utilicen la aplicación Radio Management o Radio Central pueden optar por utilizar la misma red Wi-Fi para una inscripción sencilla del dispositivo en dichas aplicaciones.

Este documento ofrece recomendaciones sobre las prácticas recomendadas relacionadas con la seguridad y el funcionamiento de la red Wi-Fi utilizada para el proceso de activación.

Recomendaciones de prácticas recomendadas para la red Wi-Fi

Asignación de dirección IP

Los dispositivos MOTOTRBO se han configurado, de forma predeterminada, para obtener una dirección IP a través de DHCP. Las siguientes recomendaciones se proporcionan para garantizar que el grupo de direcciones IP que utiliza el servicio DHCP no se agota durante la programación en bloque de dispositivos.

1. Se recomienda configurar el servidor DHCP para que emplee tiempos de concesión DHCP cortos. Esto le permite reutilizar las mismas direcciones IP a medida que se completan los lotes de radios.
2. Se recomienda configurar el servidor DHCP con una cantidad suficiente de direcciones IP para proporcionar direcciones al número de dispositivos MOTOTRBO que programará simultáneamente durante el abastecimiento en bloque, además de los demás dispositivos que estarán en la red, como Radio Management Device Programmer. Nota: Debe tener en cuenta cuándo caducará la concesión DHCP, descrita anteriormente, para permitirle reutilizar esas direcciones IP.

Detección de dispositivos MOTOTRBO (Radio Management)

Los dispositivos MOTOTRBO están configurados, de forma predeterminada, para enviar un mensaje mDNS-SD[1] al conectarse a una red Wi-Fi, y cada 90 segundos a partir de entonces. Además, Radio Management Device Programmer también envía mensajes mDNS-SD. Se proporcionan las siguientes recomendaciones para permitir que el software Radio Management detecte y lea automáticamente los dispositivos MOTOTRBO sin que el usuario deba hacer ninguna acción.

1. El número de puerto UDP para DNS-SD es el puerto 5353. La dirección IPv4 es 224.0.0.251. Las reglas del firewall de red deben permitir este número de puerto y emitir para que el servicio funcione.
2. El dispositivo MOTOTRBO y Radio Management Device Programmer deben estar en el mismo segmento de red o el tráfico de multidifusión debe reenviarse entre segmentos de red (por ejemplo, mediante una VLAN[2]). Los detalles sobre cómo configurar el equipo de red para reenviar tráfico de multidifusión se encuentran generalmente en la documentación del fabricante del equipo de red.

[1] Detección del servicio de nombres de dominio de multidifusión

[2] Red de área local virtual

Nota: El destino de detección de servicios se puede actualizar a una dirección IP de unidifusión o a un nombre de host mediante el software Radio Management.

Para obtener más información, consulte Radio Management System Planner.

Disponibilidad del servidor de tiempo de red

Los dispositivos MOTOTRBO se han configurado, de forma predeterminada, para obtener la hora actual a través del NTP[3].

Servidor NTP principal	pool.ntp.org
Servidor NTP secundario	time.google.com

Los dispositivos MOTOTRBO que se registran en certificados mediante SCEP[4] requieren una hora precisa como parte de CSR[5]. Se requiere una hora precisa para una conexión fiable al servicio en la nube central de radio.

Uso de canal Wi-Fi

Todos los dispositivos MOTOTRBO son compatibles con Wi-Fi de generación 1 (802.11b), Wi-Fi de generación 3 (802.11g) y Wi-Fi de generación 4 (802.11n).

MOTOTRBO Ion y MOTOTRBO R7 también son compatibles con Wi-Fi de generación 5 (802.11ac) y MOTOTRBO Ion también es compatible con Wi-Fi de generación 6 (802.11ax).

Se recomienda seleccionar canales Wi-Fi no superpuestos para maximizar el rendimiento de la red. En concreto, esta recomendación se aplica a los puntos de acceso Wi-Fi con cobertura superpuesta. Esto evita las interferencias de canales adyacentes entre los puntos de acceso Wi-Fi.

[3] Network Time Protocol
[4] Simple Certificate Enrollment Protocol
[5] Certificate Signing Request

En el espectro de 2,4 GHz, se recomienda seleccionar los canales 1, 6 y 11 para puntos de acceso Wi-Fi con cobertura superpuesta. Nota: Hay otras fuentes de interferencias, como los hornos microondas, que pueden interferir en el rendimiento de la red.

En el espectro de 5 GHz, hay 24 canales no superpuestos (36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161 y 165). Además, hay menos fuentes de interferencias. De forma predeterminada, algunos puntos de acceso Wi-Fi "dirigirán" los dispositivos a 5 GHz ralentizando las respuestas a 2,4 GHz.

El uso de varios puntos de acceso para aumentar el ancho de banda total disponible debe tenerse en cuenta al realizar el aprovisionamiento masivo.

Recomendaciones de prácticas recomendadas para la seguridad

El uso de una red de inscripción para separar clientes que no son de confianza de la red corporativa es una práctica recomendada. En el caso de los dispositivos MOTOTRBO, la red de inscripción inicial se encuentra activada de forma predeterminada.

SSID de la clave precompartida (PSK) de la red personal Wi-Fi: MOTOTRBO
Frase de acceso: Radio Management

Limitar el acceso físico a la red de inscripción

Se recomienda limitar el acceso físico al área de cobertura Wi-Fi de la red de inscripción a personas de confianza.

Cambiar la configuración de red Wi-Fi predeterminada

Se recomienda actualizar la red Wi-Fi y la frase de acceso a un valor distinto al predeterminado.

Redes Wi-Fi empresariales

Desde el punto de vista de la seguridad, el uso de redes Wi-Fi empresariales ofrece numerosas ventajas en comparación con las redes Wi-Fi personales. Las ventajas incluyen la capacidad de desactivar el acceso a la red en un dispositivo individual sin afectar a los demás dispositivos de la red, el cifrado exclusivo del tráfico entre el punto de acceso Wi-Fi y cada dispositivo y la capacidad de actualizar las credenciales empleadas para el cifrado mediante prácticas de administración de certificados estándar. Los dispositivos MOTOTRBO son compatibles con redes Wi-Fi personales y Wi-Fi empresariales.

Utilizar una lista de control de acceso

Se puede utilizar una lista de control de acceso (ACL) para restringir a los clientes solo a la red de inscripción y a los servidores y servicios necesarios para activar el dispositivo.

Aplicación o Servicio	Nombre de host	Puerto	Dirección	Protocolo
NTP	Pool.ntp.org time.google.com	123	Salida	UDP
DHCP	n/a (red proporcionada)	67 68	Salida Entrada	UDP
DNS	n/a (red proporcionada)	53	Salida	TCP y UDP
Protocolo de	https://devicecertmgmt-cmf21.motsolpki.com https://devicecertmgmt-cmf21.motsolpki.com	49682 49684	Salida	https
Radio Central	locator.radiocentral.motorolasolutions.com	443	Salida	https
Radio Central	Api-us.radiocentral.motorolasolutions.com Api-au.radiocentral.motorolasolutions.com	443	Salida	https
Radio Central	Usp9rmstorage.blob.core.windows.net aup9rmstorage.blob.core.windows.net	443	Salida	https
Servicio IoT	global.azure-devices-provisioning.net	443	Salida	https
Servicio IoT	iotcs-hub-us.azure-devices.net	8883	Salida Entrada	MQTT

Tabla 2: Conexiones de red del dispositivo para el proceso de activación

Historique des révisions

Révision	Date	Auteur	Description des mises à jour
Pré-édition	14/11/2021	Dan Zetzl	Projet initial.
01.00	19/11/2021	Dan Zetzl	Version 1 après intégration des commentaires de révision.
01.01	23/03/2022	Dan Zetzl	URL mises à jour dans le Tableau 2 en raison d'une erreur typographique dans l'adresse https de Radio Central et l'adresse IoT.
01.02	25/01/2023		Ajout de la langue russe.

Tableau 1 : Historique des révisions du document

Références

[1] Radio Management System Planner (System Planner pour Radio Management), MN004686A01

[2] Désactivez la mise en cache DNS côté client
https://docs.microsoft.com/fr-fr/troubleshoot/windows-client/networking/support-policy-for-dns-client-side-caching

Introduction

Les appareils MOTOTRBO Ion et R7 nécessitent une activation unique permettant d'activer les fonctions et les services logiciels souscrits avec l'appareil.

Pour simplifier l'activation unique et prendre en charge les appareils sans écran, les appareils MOTOTRBO sont livrés avec un profil de réseau Wi-Fi par défaut. En plus de l'activation unique des appareils MOTOTRBO, grâce à l'application Radio Management ou Radio Central, les clients peuvent choisir d'utiliser le même réseau Wi-Fi pour un enregistrement autonome de l'appareil dans ces applications.

Ce document présente des recommandations de meilleures pratiques relatives à la sécurité et au fonctionnement du réseau Wi-Fi utilisé pour l'activation unique.

Recommandations de meilleures pratiques pour le réseau Wi-Fi

Attribution d'adresses IP

Les appareils MOTOTRBO sont configurés par défaut pour obtenir une adresse IP via DHCP. Les recommandations suivantes sont fournies pour garantir que le pool d'adresses IP utilisé par le service DHCP n'est pas épuisé pendant la programmation en bloc des appareils.

1. Nous vous recommandons de configurer votre serveur DHCP pour qu'il utilise des durées de bail DHCP courtes. Cela vous permet de réutiliser les mêmes adresses IP au fur et à mesure que les lots de radios sont achevés.
2. Nous vous recommandons de configurer votre serveur DHCP avec une quantité suffisante d'adresses IP pour fournir des adresses à tous les appareils MOTOTRBO que vous allez programmer simultanément pendant la mise en service en bloc, ainsi que pour les autres appareils qui seront sur le réseau, tels que le programmeur d'appareils de Radio Management. Remarque : prenez en compte la durée du bail DHCP, mentionnée ci-dessus, pour pouvoir réutiliser ces adresses IP.

Détection des appareils MOTOTRBO (Radio Management)

Les appareils MOTOTRBO sont configurés par défaut pour envoyer un message mDNS-SD[1] lors de la connexion à un réseau Wi-Fi, puis toutes les 90 secondes. Le programmeur d'appareils de Radio Management envoie également des messages mDNS-SD. Les recommandations suivantes sont fournies pour permettre au logiciel Radio Management de détecter et de lire automatiquement les appareils MOTOTRBO sans que l'utilisateur ait à intervenir.

1. Le numéro de port UDP pour DNS-SD est : 5353. L'adresse IPv4 est : 224.0.0.251. Les règles du pare-feu réseau doivent autoriser ce numéro de port et la diffusion pour que le service fonctionne.
2. L'appareil MOTOTRBO et le programmeur d'appareil de Radio Management doivent se trouver sur le même segment de réseau ou le trafic multicast doit être transféré entre les segments de réseau (à l'aide d'un VLAN[2], par exemple). Vous trouverez généralement des informations sur la manière de configurer votre équipement réseau pour le transfert du trafic multicast dans la documentation produit du fabricant de votre équipement réseau.

[1] Service de nom de domaine multicast - Découverte de service
[2] Réseau local virtuel

Remarque : la destination de la découverte de service peut être mise à jour vers une adresse IP ou un nom d'hôte unicast à l'aide du logiciel Radio Management.

Veuillez vous reporter au Radio Management System Planner (System Planner pour Radio Management) pour plus de détails.

Disponibilité du serveur de synchronisation réseau (NTS)

Les appareils MOTOTRBO sont configurés par défaut pour obtenir l'heure actuelle via le protocole NTP[3].

Serveur NTP principal	pool.ntp.org
Serveur NTP secondaire	time.google.com

Les appareils MOTOTRBO qui s'inscrivent à des certificats à l'aide du SCEP[4] nécessitent une heure précise pour la CSR[5]. Pour accéder à une connexion fiable au service cloud de Radio Central, une heure précise est indispensable.

Utilisation des canaux Wi-Fi

Tous les appareils MOTOTRBO sont compatibles avec les normes de la génération Wi-Fi 1 (802.11b), la génération Wi-Fi 3 (802.11g) et la génération Wi-Fi 4 (802.11n).

MOTOTRBO Ion et MOTOTRBO R7 prennent également en charge la génération Wi-Fi 5 (802.11ac) et MOTOTRBO Ion prend aussi en charge la génération Wi-Fi 6 (802.11ax).

Nous vous recommandons de sélectionner des canaux Wi-Fi qui ne se chevauchent pas afin d'optimiser le débit sur le réseau. Plus précisément, cette recommandation s'applique aux points d'accès Wi-Fi dont les couvertures se chevauchent. En suivant cette recommandation, vous éviterez les interférences de canaux adjacents entre les points d'accès Wi-Fi.

[3] Network Time Protocol
[4] Simple Certificate Enrollment Protocol
[5] Certificate Signing Request

Dans le spectre 2,4 GHz, nous vous recommandons de sélectionner les canaux 1, 6 et 11 pour les points d'accès Wi-Fi dont les couvertures se chevauchent. Remarque : d'autres sources d'interférences, telles que les fours à micro-ondes, peuvent jouer sur les performances du réseau.

Dans le spectre 5 GHz, il existe 24 canaux sans chevauchement (36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161 et 165). De plus, les sources d'interférence sont moins nombreuses. Par défaut, certains points d'accès Wi-Fi « orientent » les appareils vers le spectre 5 GHz en ralentissant les réponses vers le spectre 2,4 GHz.

L'utilisation de plusieurs points d'accès pour augmenter la largeur de bande totale disponible est une solution à prendre en compte lors de la mise en service en bloc.

Meilleures pratiques recommandées en matière de sécurité

Nous vous recommandons d'utiliser un réseau d'inscription pour séparer les clients non fiables du réseau d'entreprise. Dans le cas des appareils MOTOTRBO, le réseau d'inscription initial est activé par défaut.

Réseau personnel Wi-Fi à clé prépartagée (PSK) SSID - MOTOTRBO
Phrase de passe : Radio Management

Limitation de l'accès physique au réseau d'inscription

Nous recommandons de limiter l'accès physique à la zone de couverture Wi-Fi du réseau d'inscription aux personnes de confiance.

Modification des paramètres par défaut du réseau Wi-Fi

Nous recommandons de mettre à jour le réseau Wi-Fi et la phrase de passe avec une valeur différente de celle par défaut.

Réseaux Wi-Fi d'entreprise

Sur le plan de la sécurité, l'utilisation de réseaux d'entreprise Wi-Fi présente plusieurs avantages par rapport aux réseaux personnels Wi-Fi. Ces avantages comprennent la possibilité de désactiver l'accès au réseau sur un appareil spécifique sans affecter les autres appareils du réseau, le cryptage unique du trafic entre le point d'accès Wi-Fi et chaque appareil, ainsi que la possibilité de mettre à jour les informations d'identification utilisées pour le cryptage à l'aide de pratiques standard de gestion des certificats. Les appareils MOTOTRBO prennent en charge les réseaux Wi-Fi personnels et d'entreprise.

Utilisation d'une liste de contrôle d'accès

Une liste de contrôle d'accès (ACL) peut être utilisée pour imposer aux clients l'utilisation du réseau d'inscription, ainsi que des serveurs et des services nécessaires pour activer l'appareil.

Service ou application	Nom d'hôte	Port	Direction	Protocole
NTP	Pool.ntp.org time.google.com	123	Sortant	UDP
DHCP	n/a (réseau fourni)	67 68	Sortant Entrant	UDP
DNS	n/a (réseau fourni)	53	Sortant	TCP et UDP
Gestion des certificats	https://devicecertmgmt-cmf21.motsolpki.com https://devicecertmgmt-cmf21.motsolpki.com	49682 49684	Sortant	https
Radio Central	locator.radiocentral.motorolasolutions.com	443	Sortant	https
Radio Central	Api-us.radiocentral.motorolasolutions.com Api-au.radiocentral.motorolasolutions.com	443	Sortant	https
Radio Central	Usp9rmstorage.blob.core.windows.net aup9rmstorage.blob.core.windows.net	443	Sortant	https

Service ou application	Nom d'hôte	Port	Direction	Protocole
Service IoT	global.azure-devices-provisioning.net	443	Sortant	https
Service IoT	iotcs-hub-us.azure-devices.net	8883	Sortant Entrant	MQTT

Tableau 2 : Connexions au réseau de l'appareil pour une activation unique

Cronologia delle revisioni

Revisione	Data	Autore	Descrizione degli aggiornamenti
Versione preliminare	14 novembre 2021	Dan Zetzl	Bozza iniziale
01.00	19 novembre 2021	Dan Zetzl	Versione uno dopo aver inserito i commenti della revisione.
01.01	23 marzo 2022	Dan Zetzl	URL aggiornati nella Tabella 2 per un refuso nella voce https di Radio Central e nell'indirizzo IoT.
01.02	25 gennaio 2023		Aggiunta della lingua russa.

Tabella 1: Cronologia delle revisioni del documento

Bibliografia

[1] Radio Management System Planner, MN004686A01

[2] Disabilitazione del caching DNS lato client, https://docs.microsoft.com/en-us/windows-server/networking/dns/troubleshoot/disable-dns-client-side-caching

Introduzione

I dispositivi MOTOTRBO Ion e R7 richiedono un'attivazione una tantum per abilitare le funzionalità e i servizi software acquistati con essi.

Per semplificare l'attivazione una tantum e supportare i dispositivi senza display, i dispositivi MOTOTRBO vengono forniti con un profilo di rete Wi-Fi predefinito. Oltre all'attivazione una tantum dei dispositivi MOTOTRBO, i clienti che utilizzano l'applicazione Radio Management o Radio Central possono scegliere di utilizzare la stessa rete Wi-Fi per la registrazione zero-touch del dispositivo in tali applicazioni.

Questo documento fornisce raccomandazioni sulle best practice relative alla sicurezza e al funzionamento della rete Wi-Fi utilizzata per l'attivazione una tantum.

Raccomandazioni sulle best practice per la rete Wi-Fi

Assegnazione dell'indirizzo IP

I dispositivi MOTOTRBO sono configurati, per impostazione predefinita, per ottenere un indirizzo IP tramite DHCP. Le seguenti raccomandazioni sono fornite per garantire che il pool di indirizzi IP utilizzati dal servizio DHCP non venga consumato durante la programmazione in blocco dei dispositivi.

1. Si consiglia di configurare il server DHCP in modo che utilizzi tempi di allocazione DHCP brevi. In questo modo è possibile riutilizzare gli stessi indirizzi IP al completamento dei batch di radio.
2. Si consiglia di configurare il server DHCP con una quantità sufficiente di indirizzi IP per fornire indirizzi al numero di dispositivi MOTOTRBO che verranno programmati contemporaneamente durante il provisioning in blocco e agli altri dispositivi che saranno sulla rete, ad esempio Radio Management Device Programmer. Nota: è necessario tenere conto della scadenza dell'allocazione DHCP, descritta in precedenza, per consentire di riutilizzare tali indirizzi IP.

MOTOTRBO Device Discovery (Radio Management)

I dispositivi MOTOTRBO sono configurati, per impostazione predefinita, per inviare un messaggio mDNS-SD[1] durante la connessione a una rete Wi-Fi e, successivamente, ogni 90 secondi. Anche Radio Management Device Programmer invia messaggi mDNS-SD. I seguenti suggerimenti consentono al software Radio Management di rilevare e leggere automaticamente i dispositivi MOTOTRBO senza alcuna azione richiesta dall'utente.

1. Il numero di porta UDP per DNS-SD è 5353. L'indirizzo IPv4 è 224.0.0.251. Le regole del firewall di rete devono consentire questo numero di porta e la trasmissione affinché il servizio funzioni.
2. Il dispositivo MOTOTRBO e Radio Management Device Programmer devono trovarsi sullo stesso segmento di rete oppure il traffico multicast deve essere inoltrato tra segmenti di rete (ad esempio, utilizzando una VLAN[2]). I dettagli sulla modalità di configurazione delle apparecchiature di rete per inoltrare il traffico multicast sono, in genere, disponibili nella documentazione del prodotto fornito dal produttore delle apparecchiature.

[1] Individuazione servizio nomi dominio multicast
[2] Virtual Local Area Network

Nota: la destinazione di individuazione del servizio può essere aggiornata con un IP o nome host unicast utilizzando il software Radio Management.

Per ulteriori dettagli, fare riferimento a Radio Management System Planner.

Disponibilità del server di riferimento orario di rete

I dispositivi MOTOTRBO sono configurati, per impostazione predefinita, per ottenere l'ora corrente tramite NTP[3].

Server NTP primario	pool.ntp.org
Server NTP secondario	time.google.com

La registrazione dei dispositivi MOTOTRBO per i certificati che utilizzano SCEP[4] richiede un tempo preciso come parte del CSR[5]. Per una connessione affidabile al servizio cloud di Radio Central, è necessario un tempo preciso.

Utilizzo del canale Wi-Fi

Tutti i dispositivi MOTOTRBO supportano la generazione Wi-Fi 1 (802.11b), la generazione Wi-Fi 3 (802.11g) e la generazione Wi-Fi 4 (802.11n).

MOTOTRBO Ion e MOTOTRBO R7 supportano anche la generazione Wi-Fi 5 (802.11ac) e MOTOTRBO Ion supporta anche la generazione Wi-Fi 6 (802.11ax).

È consigliabile selezionare canali Wi-Fi non sovrapposti per massimizzare il throughput sulla rete. In particolare, questa raccomandazione si applica agli access point Wi-Fi con copertura sovrapposta. In questo modo si evita l'interferenza dei canali adiacenti tra i punti di accesso Wi-Fi.

[3] Network Time Protocol
[4] Simple Certificate Enrollment Protocol
[5] Certificate Signing Request

Nello spettro a 2,4 GHz, si consiglia di selezionare i canali 1, 6 e 11 per gli access point Wi-Fi con copertura sovrapposta. Nota: altre fonti di interferenza, come i forni a microonde, possono interferire con le prestazioni della rete.

Nello spettro a 5 GHz, sono presenti 24 canali non sovrapposti (36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161 e 165). Inoltre, sono presenti meno fonti di interferenza. Per impostazione predefinita, alcuni access point Wi-Fi "indirizzano" i dispositivi verso lo spettro a 5 GHz, rallentando le risposte allo spettro a 2,4 GHz.

Quando si esegue il provisioning in blocco, è necessario prendere in considerazione l'utilizzo di più access point per aumentare la larghezza di banda totale disponibile.

Raccomandazioni sulle best practice per la sicurezza

Si consiglia di utilizzare una rete di registrazione per separare i client non attendibili dalla rete aziendale. Nel caso di dispositivi MOTOTRBO, la rete di registrazione iniziale è attivata per impostazione predefinita.

SSID con chiave pre-condivisa (PSK) per rete personale Wi-Fi - MOTOTRBO
Passphrase: Radio Management

Limitare l'accesso fisico alla rete di registrazione

Si consiglia di limitare l'accesso fisico all'area di copertura Wi-Fi della rete di registrazione a persone attendibili.

Modificare le impostazioni di rete Wi-Fi predefinite

Si consiglia di aggiornare la rete Wi-Fi e la passphrase con un valore diverso da quello predefinito.

Reti Wi-Fi aziendali

Dal punto di vista della sicurezza, l'uso delle reti Wi-Fi aziendali offre diversi vantaggi rispetto alle reti personali Wi-Fi. I vantaggi includono la possibilità di disabilitare l'accesso alla rete su un singolo dispositivo senza influire sugli altri dispositivi della rete, che il traffico venga crittografato in modo univoco tra il punto di accesso Wi-Fi e ciascun dispositivo e la possibilità di aggiornare le credenziali utilizzate per la crittografia utilizzando le procedure standard di gestione dei certificati. I dispositivi MOTOTRBO supportano sia le reti Wi-Fi personali che le rete Wi-Fi aziendali.

Utilizzo di un elenco di controllo degli accessi

È possibile utilizzare un elenco di controllo degli accessi (ACL) per limitare i client solo alla rete di registrazione e ai server e ai servizi necessari per attivare il dispositivo.

Applicazione o servizio	Nome host	Porta	Direzione	Protocollo
NTP	Pool.ntp.org time.google.com	123	In uscita	UDP
DHCP	n/d (rete fornita)	67 68	In uscita In entrata	UDP
DNS	n/d (rete fornita)	53	In uscita	TCP E UDP
Gestione dei certificati	https://devicecertmgmt-cmf21.motsolpki.com https://devicecertmgmt-cmf21.motsolpki.com	49682 49684	In uscita	https
Radio Central	locator.radiocentral.motorolasolutions.com	443	In uscita	https
Radio Central	Api-us.radiocentral.motorolasolutions.com Api-au.radiocentral.motorolasolutions.com	443	In uscita	https
Radio Central	Usp9rmstorage.blob.core.windows.net aup9rmstorage.blob.core.windows.net	443	In uscita	https
Servizio IoT	global.azure-devices-provisioning.net	443	In uscita	https
Servizio IoT	iotcs-hub-us.azure-devices.net	8883	In uscita In entrata	MQTT

Tabella 2: Connessioni di rete del dispositivo per l'attivazione una tantum

Historia zmian

Wersja	Data	Autor	Opis aktualizacji
Przedpremierowe	14.11.2021 r.	Dan Zetzl	Wstępna wersja robocza.
01.00	19.11.2021 r.	Dan Zetzl	Wersja pierwsza po uwzględnieniu uwag z przeglądu.
01.01	23.03.2022 r.	Dan Zetzl	Zaktualizowano adresy URL w tabeli 2 w związku z literówką we wpisie Radio Central https i adresie IoT.
01.02	25.01.2023 r.		Dodano język rosyjski.

Tabela 1: Historia zmian dokumentu

Referencje

[1] Narzędzie planowania systemu Radio Management, MN004686A01

[2] Wyłączanie pamięci podręcznej po stronie klienta DNS, https://docs.microsoft.com/en-us/windows-server/networking/dns/troubleshoot/disable-dns-client-side-caching

Wprowadzenie

Urządzenia MOTOTRBO Ion i R7 wymagają jednorazowej aktywacji w celu włączenia funkcji oprogramowania i usług zakupionych z urządzeniem.

W celu uproszczenia jednorazowej aktywacji i wsparcia urządzeń bez wyświetlacza urządzenia MOTOTRBO są dostarczane z domyślnym profilem sieci Wi-Fi. Oprócz jednorazowej aktywacji urządzeń MOTOTRBO klienci korzystający z aplikacji Radio Management lub Radio Central mogą używać rejestracji bezdotykowej urządzenia w tych aplikacjach.

Niniejszy dokument zawiera zalecenia dotyczące najlepszych praktyk bezpieczeństwa i eksploatacji sieci Wi-Fi używanej do jednorazowej aktywacji.

Zalecenia dotyczące najlepszych praktyk dla sieci Wi-Fi

Przydzielanie adresu IP

Urządzenia MOTOTRBO są domyślnie skonfigurowane do uzyskiwania adresu IP przez DHCP. Poniższe zalecenia zostały przedstawione dla uniknięcia wyczerpania puli adresów IP używanych przez usługę DHCP podczas zbiorczego programowania urządzeń.

1. Zalecane jest skonfigurowanie serwera DHCP do używania krótkich czasów dzierżawy DHCP. Umożliwia to ponowne wykorzystanie tych samych adresów IP, co dla zakończonych partii radiotelefonów.
2. Zalecane jest skonfigurowanie na serwerze DHCP wystarczającej ilości adresów IP dla zapewnienia adresów dla liczby urządzeń MOTOTRBO, które będą programowane jednocześnie podczas konfiguracji zbiorczej oraz innych urządzeń, które będą w sieci, takich jak programator urządzeń Radio Management. Uwaga: wygaśnięcie omówionej wyżej dzierżawy DHCP umożliwi ponowne wykorzystanie adresów IP.

Wykrywanie urządzeń MOTOTRBO (Radio Management)

Urządzenia MOTOTRBO są domyślnie skonfigurowane do wysyłania komunikatu mDNS-SD[1] podczas łączenia z siecią Wi-Fi i co 90 sekund później. Ponadto programator radiotelefonów Radio Management wysyła komunikaty mDNS-SD. Poniższe zalecenia zostały przedstawione w celu umożliwienia oprogramowaniu Radio Management automatycznego wykrywania I odczytywania urządzeń MOTOTRBO bez wymaganych działań użytkownika.

1. Numer portu UDP dla DNS-SD to 5353. Adres IPv4 to 224.0.0.251. Reguły zapory muszą zezwalać na ten numer portu i nadawanie, aby usługa działała.
2. Urządzenie MOTOTRBO i programator urządzeń muszą być w tym samym segmencie sieci lub ruch multicast musi być przekazywany między segmentami sieci (np. przy użyciu VLAN[2]). Szczegóły dotyczące konfiguracji urządzeń sieciowych do przekazywania ruchu multicast można zwykle znaleźć w literaturze produktu producenta urządzeń sieciowych.

[1] Wykrywanie usług nazwy domeny Multicast
[2] Wirtualna sieć lokalna

Uwaga: miejsce docelowe wykrywania usług można zaktualizować na adres IP lub nazwę hosta unicast przy użyciu oprogramowania Radio Management.

Więcej informacji można znaleźć w sekcji Narzędzie planowania systemu Radio Management.

Dostępność sieciowego serwera czasu

Urządzenia MOTOTRBO są domyślnie skonfigurowane do uzyskiwania bieżącego czasu przez NTP[3].

Podstawowy serwer NTP	pool.ntp.org
Dodatkowy serwer NTP	time.google.com

Urządzenia MOTOTRBO rejestrowane w certyfikatach przy użyciu SCEP[4] wymagają dokładnego czasu w ramach CSR[5]. Dokładny czas jest wymagany dla niezawodnego połączenia z usługą chmury Radio Central.

Wykorzystanie kanału Wi-Fi

Wszystkie urządzenia MOTOTRBO wspierają Wi-Fi generacji 1 (802.11b), Wi-Fi generacji 3 (802.11g) i Wi-Fi generacji 4 (802.11n).

MOTOTRBO Ion i MOTOTRBO R7 wspierają także Wi-Fi generacji 5 (802.11ac), MOTOTRBO Ion wspierają także Wi-Fi generacji 6 (802.11ax).

Najlepszą praktyką jest wybieranie nienakładających się kanałów Wi-Fi w celu uzyskania maksymalnej przepustowości w sieci. Zalecenie to dotyczy w szczególności punktów dostępu Wi-Fi z nakładającym się zasięgiem. Umożliwia to uniknięcie zakłóceń sąsiedniego kanału między punktami dostępu Wi-Fi.

[3] Network Time Protocol
[4] Simple Certificate Enrollment Protocol
[5] Certificate Signing Request

W spektrum 2,4 GHz zalecane jest wybieranie kanałów 1, 6 i 11 dla punktów dostępu Wi-Fi z nakładającym się zasięgiem. Uwaga: inne źródła zakłóceń, takie jak kuchenki mikrofalowe, mogą zakłócać działanie sieci.

W spektrum 5 GHz znajdują się 24 nienakładające się kanały (36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161 i 165). Ponadto będzie mniej źródeł zakłóceń. Domyślnie niektóre punkty dostępu Wi-Fi „kierują” urządzenia do 5 GHz poprzez spowolnienie odpowiedzi na 2,4 GHz.

Wykorzystanie wielu punktów dostępu w celu zwiększenia całkowitej dostępnej przepustowości należy uwzględnić podczas konfiguracji zbiorczej.

Zalecenia dotyczące najlepszych praktyk dla bezpieczeństwa

Wykorzystanie sieci rejestracji do oddzielania klientów niezaufanych od sieci korporacyjnej jest zalecaną najlepszą praktyką. W przypadku urządzeń MOTOTRBO sieć rejestracji wstępnej jest domyślnie włączona.

SSID osobistego wstępnego klucza sieciowego Wi-Fi (PSK) – MOTOTRBO
Hasło: Radio Management

Ograniczenie dostępu fizycznego do sieci rejestracji

Zalecaną najlepszą praktyką jest zastrzeżenie dostępu fizycznego do obszaru zasięgu Wi-Fi sieci rejestracji dla osób zaufanych.

Zmiana ustawień domyślnych sieci Wi-Fi

Zalecaną najlepszą praktyką jest aktualizacja sieci Wi-Fi i hasła na wartości inne niż domyślne.

Firmowe sieci Wi-Fi

Z punktu widzenia bezpieczeństwa wykorzystanie firmowych sieci Wi-Fi zapewnia wiele zalet w porównaniu z osobistymi sieciami Wi-Fi. Zalety obejmują możliwość wyłączania dostępu do sieci na poziomie indywidualnego urządzenia bez wpływu na inne urządzenia w sieci, unikalne szyfrowanie ruchu między punktem dostępu Wi-Fi a każdym urządzeniem i możliwość aktualizacji danych uwierzytelniających wykorzystujących standardowe praktyki zarządzania certyfikatami. Urządzenia MOTOTRBO wspierają osobiste sieci Wi-Fi i firmowe sieci Wi-Fi.

Korzystanie z listy kontroli dostępu

Lista kontroli dostępu (ACL) umożliwia ograniczanie dostępu klientów tylko do sieci rejestracji oraz serwerów i usług wymaganych do aktywacji urządzenia.

Aplikacja lub usługa	Nazwa hosta	Port	Kierunek	Protokół
NTP	Pool.ntp.org time.google.com	123	Dla ruchu wychodzącego	UDP
DHCP	nd. (konfiguracja sieci)	67 68	Dla ruchu wychodzącego Dla ruchu przychodzącego	UDP
DNS	nd. (konfiguracja sieci)	53	Dla ruchu wychodzącego	TCP i UDP
Zarządzanie certyfikatami	https://devicecertmgmt-cmf21.motsolpki.com https://devicecertmgmt-cmf21.motsolpki.com	49682 49684	Dla ruchu wychodzącego	https
Radio Central	locator.radiocentral.motorolasolutions.com	443	Dla ruchu wychodzącego	https
Radio Central	Api-us.radiocentral.motorolasolutions.com Api-au.radiocentral.motorolasolutions.com	443	Dla ruchu wychodzącego	https
Radio Central	Usp9rmstorage.blob.core.windows.net aup9rmstorage.blob.core.windows.net	443	Dla ruchu wychodzącego	https
Usługa IoT	global.azure-devices-provisioning.net	443	Dla ruchu wychodzącego	https
Usługa IoT	iotcs-hub-us.azure-devices.net	8883	Dla ruchu wychodzącego Dla ruchu przychodzącego	MQTT

Tabela 2: Połączenia sieciowe urządzeń do jednorazowej aktywacji

История редакций документации

Редакция	Дата	Автор	Описание обновлений
Предварительный выпуск	14 ноября 2021 г.	Дэн Зецл	Исходный черновик.
01.00	19 ноября 2021 г.	Дэн Зецл	Первый выпуск после проверки внесенных комментариев.
01.01	23 марта 2022 г.	Дэн Зецл	Обновлены URL-адреса в Таблице 2 из-за опечатки в информации о протоколе HTTPS для RadioCentral и адресе службы "Интернет вещей".
01.02	25 января 2023 г.		Добавлен русский язык.

Таблица 1. История редакций документа

Справочные материалы

[1] Системный планировщик Radio Management, MN004686A01

[2] Отключение кэширования на стороне клиента DNS, https://docs.microsoft.com/en-us/windows-server/networking/dns/troubleshoot/disable-dns-client-side-caching

Введение

Для устройств MOTOTRBO Ion и R7 требуется единовременная активация программных функций и служб, приобретенных вместе с устройством.

Для упрощения единовременной активации и поддержки устройств без дисплея устройства MOTOTRBO поставляются с профилем сети Wi-Fi по умолчанию. Помимо единовременной активации устройств MOTOTRBO клиенты, использующие приложение Radio Management или RadioCentral, могут использовать ту же сеть Wi-Fi для автоматической регистрации устройства в этих приложениях.

В этом документе приведены рекомендации по обеспечению безопасности и работе с сетью Wi-Fi, используемой для единовременной активации.

Рекомендации по использованию сети Wi-Fi

Назначение IP-адреса

По умолчанию на устройствах MOTOTRBO настроено получение IP-адреса с помощью DHCP. Ниже приведены рекомендации по обеспечению того, чтобы пул IP-адресов, используемых службой DHCP, не был исчерпан при программировании устройств в пакетном режиме.

1. Рекомендуется настроить на сервере DHCP использование короткого периода аренды DHCP. Это позволяет повторно использовать те же IP-адреса при заполнении пакетов радиостанций.
2. Рекомендуется настроить на сервере DHCP достаточное количество IP-адресов для их предоставления большому количеству устройств MOTOTRBO, программирование которых будет выполняться одновременно при подготовке к работе в пакетном режиме, а также другим устройствам, которые будут находиться в сети, например программатору устройств Radio Management. Примечание: необходимо учитывать, когда истекает срок аренды DHCP, упомянутый выше, чтобы повторно использовать эти IP-адреса.

Обнаружение устройств MOTOTRBO (Radio Management)

По умолчанию на устройствах MOTOTRBO настроена отправка сообщения mDNS-SD[1] при подключении к сети Wi-Fi и каждые 90 сек. после этого. Программатор устройств Radio Management также отправляет сообщения mDNS-SD. Ниже приведены рекомендации, которые позволяют программному обеспечению Radio Management автоматически обнаруживать устройства MOTOTRBO и считывать их данные без каких-либо действий со стороны пользователя.

1. Номер порта UDP для DNS-SD — порт 5353. Адрес IPv4 — 224.0.0.251. Правила сетевого брандмауэра должны разрешать этот номер порта и широковещательную передачу, чтобы обеспечить возможность работы службы.
2. Устройство MOTOTRBO и программатор устройств Radio Management должны находиться в одном сегменте сети, или трафик многоадресного вещания должен перенаправляться между сегментами сети (например, с помощью VLAN[2]). Подробные сведения о настройке на сетевом оборудовании перенаправления трафика многоадресного вещания можно найти в документации производителя сетевого оборудования.

[1] Multicast Domain Name System Service Discovery
[2] Виртуальная локальная компьютерная сеть

Примечание. Назначение обнаружения службы можно обновить до индивидуального IP-адреса или имени хоста с помощью программного обеспечения Radio Management.

Для получения подробной информации см. Системный планировщик Radio Management.

Доступность сервера сетевого времени

По умолчанию на устройствах MOTOTRBO настроено получение текущего времени с помощью NTP[3].

Основной сервер NTP	pool.ntp.org
Дополнительный сервер NTP	time.google.com

Для регистрации устройств MOTOTRBO с целью получения сертификатов с помощью SCEP[4] требуется точное время в рамках CSR[5]. Точное время требуется для надежного подключения к облачному сервису RadioCentral.

Использование канала Wi-Fi

Все устройства MOTOTRBO поддерживают Wi-Fi 1-го поколения (802.11b), Wi-Fi 3-го поколения (802.11g) и Wi-Fi 4-го поколения (802.11n).

Кроме того, MOTOTRBO Ion и MOTOTRBO R7 поддерживают Wi-Fi 5-го поколения (802.11ac), а MOTOTRBO Ion также поддерживает Wi-Fi 6-го поколения (802.11ax).

Рекомендуется выбирать неперекрывающиеся каналы Wi-Fi для максимального увеличения пропускной способности сети. В частности, эта рекомендация относится к точкам доступа Wi-Fi с перекрывающимися зонами покрытия. Это позволяет избежать помех от соседних каналов между точками доступа Wi-Fi.

[3] Network Time Protocol
[4] Simple Certificate Enrollment Protocol
[5] Certificate Signing Request

В диапазоне 2,4 ГГц рекомендуется выбрать каналы 1, 6 и 11 для точек доступа Wi-Fi с перекрывающимися зонами покрытия. Примечание: на работу сети могут влиять другие источники помех, например микроволновые печи.

В диапазоне 5 ГГц доступно 24 неперекрывающихся канала (36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161 и 165). Кроме того, в нем меньше источников помех. По умолчанию некоторые точки доступа Wi-Fi "направляют" устройства на диапазон 5 ГГц, замедляя отклики в диапазоне 2,4 ГГц.

При подготовке к работе в пакетном режиме следует рассмотреть возможность использования нескольких точек доступа для увеличения общей доступной полосы пропускания.

Рекомендации по обеспечению безопасности

Рекомендуется использовать сеть с регистрацией для защиты корпоративной сети от недоверенных клиентов. В случае устройств MOTOTRBO сеть с начальной регистрацией включена по умолчанию.

SSID общего ключа (PSK) персональной сети Wi-Fi: MOTOTRBO
Парольная фраза: Radio Management

Ограничение физического доступа к сети с регистрацией

Рекомендуется ограничить физический доступ к зоне покрытия Wi-Fi в сети с регистрацией доверенными лицами.

Изменение настроек сети Wi-Fi по умолчанию

Рекомендуется настроить новые сеть Wi-Fi и парольную фразу, отличные от значений по умолчанию.

Корпоративные сети Wi-Fi

С точки зрения безопасности использование корпоративных сетей Wi-Fi обеспечивает ряд преимуществ по сравнению с персональными сетями Wi-Fi. К преимуществам относится возможность отключать доступ к сети на отдельных устройствах без затрагивания других устройств в сети, уникальные методы шифрования трафика между точкой доступа Wi-Fi и каждым устройством, а также возможность обновления учетных данных, используемых для шифрования, с помощью стандартных практик управления сертификатами. Устройства MOTOTRBO поддерживают как персональные, так и корпоративные сети Wi-Fi.

Использование списка контроля доступа

Список контроля доступа (ACL) можно использовать для ограничения клиентов только сетью с регистрацией, а также серверами и службами, необходимыми для активации устройства.

Приложение или служба	Имя хоста	Порт	Направление	Протокол
NTP	Pool.ntp.org time.google.com	123	Исходящее	UDP
DHCP	Н/д (предоставляется сетью)	67 68	Исходящее Входящее	UDP
DNS	Н/д (предоставляется сетью)	53	Исходящее	TCP и UDP
Управление сертификатами	https://devicecertmgmt-cmf21.motsolpki.com https://devicecertmgmt-cmf21.motsolpki.com	49682 49684	Исходящее	HTTPS
RadioCentral	locator.radiocentral.motorolasolutions.com	443	Исходящее	HTTPS
RadioCentral	Api-us.radiocentral.motorolasolutions.com Api-au.radiocentral.motorolasolutions.com	443	Исходящее	HTTPS
RadioCentral	Usp9rmstorage.blob.core.windows.net aup9rmstorage.blob.core.windows.net	443	Исходящее	HTTPS
Служба "Интернет вещей"	global.azure-devices-provisioning.net	443	Исходящее	HTTPS
Служба "Интернет вещей"	iotcs-hub-us.azure-devices.net	8883	Исходящее Входящее	MQTT

Таблица 2. Сетевые подключения устройств для единовременной активации

Revizyon Geçmişi

Revizyon	Tarih	Yazar	Güncellemelerin Açıklaması
Yayın Öncesi Eğitim	14.11.2021	Dan Zetzl	İlk Taslak.
01.00	19.11.2021	Dan Zetzl	İnceleme yorumları eklendikten sonraki ilk yayın.
01.01	23.03.2022	Dan Zetzl	Tablo 2'deki URL'ler Radyo Central https girişi ve IoT adresinde yazım hatası için güncellendi.
01.02	25.01.2023		Rusça eklendi.

Tablo 1: Belge Revizyon Geçmişi

Referanslar

[1] Telsiz Yönetimi Sistem Planlayıcı, MN004686A01

[2] DNS İstemci Tarafı Önbelleğe Almayı Devre Dışı Bırakma, https://docs.microsoft.com/en-us/windows-server/networking/dns/troubleshoot/disable-dns-client-side-caching

Giriş

MOTOTRBO Ion ve R7 cihazları, yazılım özelliklerinin ve cihazla birlikte satın alınan hizmetlerin kullanılabilmesi için tek seferlik etkinleştirme gerektirir.

Tek seferlik etkinleştirmeyi basitleştirmek ve ekransız cihazları desteklemek için MOTOTRBO cihazları, varsayılan bir Wi-Fi ağı profiliyle gönderilir. MOTOTRBO cihazlarının tek seferlik etkinleştirilmesine ek olarak, Telsiz Yönetimi veya Radio Central uygulamasını kullanan müşteriler cihazın bu uygulamalara kaydını ekran kullanmadan gerçekleştirebilmek için aynı Wi-Fi ağını kullanmayı tercih edebilir.

Bu belge, tek seferlik etkinleştirme için kullanılan Wi-Fi ağının güvenliği ve çalışması ile ilgili en iyi uygulama önerilerini sunar.

Wi-Fi Ağı İçin En İyi Uygulama Önerileri

IP Adresi Atama

MOTOTRBO cihazları, varsayılan olarak DHCP üzerinden bir IP adresi almak üzere yapılandırılır. Cihazların toplu olarak programlanması sırasında DHCP hizmeti tarafından kullanılan IP adresi havuzunun tükenmemesi için aşağıdaki öneriler verilmiştir.

1. DHCP sunucunuzu, kısa DHCP kiralama süreleri kullanacak şekilde yapılandırmanız önerilir. Bu, telsiz grupları tamamlandıkça aynı IP adreslerini yeniden kullanmanıza olanak tanır.
2. Toplu provizyon sırasında eş zamanlı olarak programlayacağınız MOTOTRBO cihazlarına ve Telsiz Yönetimi Cihaz Programlayıcısı gibi ağda yer alacak diğer cihazlara adres sağlamak için DHCP sunucunuzu yeterli miktarda IP adresi ile yapılandırmanız önerilir. Not: Bu IP adreslerini yeniden kullanabilmeniz için yukarıda bahsedilen DHCP kiralama süresinin ne zaman dolacağını dikkate almanız gerekir.

MOTOTRBO Cihazı Keşfi (Telsiz Yönetimi)

MOTOTRBO cihazları, varsayılan olarak, bir Wi-Fi ağına bağlanırken ve bundan sonraki her 90 saniyede bir mDNS-SD[1] mesajı göndermek üzere yapılandırılır. Telsiz Yönetimi Cihazı Programlayıcısı da mDNS-SD mesajları gönderir. Telsiz Yönetimi yazılımının MOTOTRBO cihazlarını kullanıcı tarafından herhangi bir işlem yapılması gerekmeden otomatik olarak keşfetmesini ve okumasını sağlamak için aşağıdakiler önerilmektedir.

1. DNS-SD için UDP bağlantı noktası numarası, 5353 numaralı bağlantı noktasıdır. IPv4 adresi 224.0.0.251'dir. Hizmetin çalışması için ağ güvenlik duvarı kuralları, bu bağlantı noktası numarasının ve yayının kullanılmasına izin vermelidir.
2. MOTOTRBO cihazı ve Telsiz Yönetimi Cihaz Programlayıcısı aynı ağ segmentinde olmalıdır veya çoklu gönderim yayını trafiği ağ segmentleri arasında iletilmelidir (örneğin VLAN[2] kullanılarak). Ağ ekipmanınızı nasıl çoklu gönderim yayını trafiğini iletecek şekilde yapılandıracağınıza ilişkin ayrıntılar genellikle ağ ekipmanı üreticinizin sağladığı ürün bilgilerinde bulunabilir.

[1] Çoklu Gönderim Yayını Etki Alanı Adı Hizmeti Hizmet Keşfi
[2] Sanal Yerel Alan Ağı

Not: Hizmet keşfi hedefi, Telsiz Yönetimi yazılımı kullanılarak tek yönlü yayın IP'si veya ana bilgisayar adı olarak güncellenebilir.

Daha fazla ayrıntı için lütfen Telsiz Yönetimi Sistem Planlayıcısına başvurun.

Ağ Zaman Sunucusu Kullanılabilirliği

MOTOTRBO cihazları, varsayılan olarak NTP[3] üzerinden geçerli saati alacak şekilde yapılandırılır.

Birincil NTP Sunucusu	pool.ntp.org
İkincil NTP Sunucusu	time.google.com

SCEP[4] kullanarak sertifika kaydı yapılan MOTOTRBO cihazları için CSR[5] bağlamında zamanın doğru olması gerekir. Radio Central bulut hizmeti ile güvenilir bir bağlantı sağlanması için zaman doğru olmalıdır.

Wi-Fi Kanalı Kullanımı

Tüm MOTOTRBO cihazları Wi-Fi 1. Nesil (802.11b), Wi-Fi 3. Nesil (802.11g) ve Wi-Fi 4. Nesil (802.11n) desteğine sahiptir.

MOTOTRBO Ion ve MOTOTRBO R7 ayrıca Wi-Fi 5. Nesil (802.11ac) ve MOTOTRBO Ion ek olarak Wi-Fi 6. Nesil (802.11ax) desteğine sahiptir.

Ağdaki verimi en üst düzeye çıkarmak için çakışmayan Wi-Fi kanallarını seçmek en iyi uygulamadır. Bu öneri özellikle çakışan kapsama alanlarına sahip Wi-Fi erişim noktaları için geçerlidir. Bu, Wi-Fi erişim noktaları arasındaki yan kanal parazitini önler.

[3] Ağ Zaman Protokolü
[4] Basit Sertifika Kayıt Protokolü
[5] Sertifika Onay İsteği

2,4 GHz spektrumunda, çakışan kapsama alanlarına sahip Wi-Fi erişim noktaları için 1, 6 ve 11 numaralı kanalları seçmeniz önerilir. Not: Mikrodalga fırınlar gibi diğer parazit kaynakları ağ performansını etkileyebilir.

5 GHz spektrumunda, çakışmayan 24 kanal mevcuttur (36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161 ve 165). Ayrıca daha az parazit kaynağı vardır. Varsayılan olarak bazı Wi-Fi erişim noktaları, 2,4 GHz'e verilen yanıtları yavaşlatarak cihazları 5 GHz'e "yönlendirir".

Toplu hazırlama işlemi sırasında, toplam kullanılabilir bant genişliğini artırmak için birden fazla erişim noktasının kullanılması düşünülmelidir.

Güvenlikle İlgili En İyi Uygulama Önerileri

Güvenilir olmayan istemcileri kurumsal ağdan ayırmak için bir kayıt ağının kullanılması en iyi uygulama olarak önerilir. MOTOTRBO cihazlarında, ilk kayıt ağı varsayılan olarak etkinleştirilir.

Wi-Fi Kişisel Ağ Önceden Paylaşılan Anahtar (PSK) SSID - MOTOTRBO
Parola: Telsiz Yönetimi

Kayıt Ağına Fiziksel Erişimi Sınırlama

Kayıt ağının Wi-Fi kapsama alanına fiziksel erişimi güvenilen kişilerle sınırlamak en iyi uygulama olarak önerilir.

Varsayılan Wi-Fi Ağı Ayarlarını Değiştirme

Varsayılan değeri değiştirerek Wi-Fi ağı ve parolayı güncellemek en iyi uygulama olarak önerilir.

Kurumsal Wi-Fi Ağları

Güvenlik açısından bakıldığında Kurumsal Wi-Fi ağları, kişisel Wi-Fi ağlarına kıyasla birçok avantaj sağlar. Bu avantajlar arasında ağdaki diğer cihazları etkilemeden tek bir cihaz bazında ağ erişimini devre dışı bırakma özelliği, Wi-Fi erişim noktası ve her bir cihaz arasındaki trafiğin benzersiz şekilde şifrelenmesi ve standart sertifika yönetimi uygulamalarını kullanarak şifreleme için kullanılan kimlik bilgilerini güncelleme özelliği bulunur. MOTOTRBO cihazları hem Wi-Fi Kişisel hem de Wi-Fi Kurumsal ağlarını destekler.

Erişim Denetim Listesi Kullanma

İstemcileri yalnızca kayıt ağı ve cihazı etkinleştirmek için gereken sunucular ve hizmetlerle sınırlamak için bir Erişim Denetim Listesi (ACL) kullanılabilir.

Uygulama veya Hizmet	Ana Bilgisayar Adı	Port	Yön	Protokol
NTP	Pool.ntp.org time.google.com	123	Giden	UDP
DHCP	Yok (ağ tarafından sağlanır)	67 68	Giden Gelen	UDP
DNS	Yok (ağ tarafından sağlanır)	53	Giden	TCP ve UDP
Sertifika Yönetimi	https://devicecertmgmt-cmf21.motsolpki.com https://devicecertmgmt-cmf21.motsolpki.com	49682 49684	Giden	https
Radio Central	locator.radiocentral.motorolasolutions.com	443	Giden	https
Radio Central	Api-us.radiocentral.motorolasolutions.com Api-au.radiocentral.motorolasolutions.com	443	Giden	https
Radio Central	Usp9rmstorage.blob.core.windows.net aup9rmstorage.blob.core.windows.net	443	Giden	https
IoT Hizmeti	global.azure-devices-provisioning.net	443	Giden	https
IoT Hizmeti	iotcs-hub-us.azure-devices.net	8883	Giden Gelen	MQTT

Tablo 2: Tek seferlik Etkinleştirme İçin Cihaz Ağ Bağlantıları

المراجعة السابقة

المراجعة	التاريخ	المؤلف	وصف التحديثات
قبل الإصدار	2021/11/14	Dan Zetzl	المسودة الأولية.
01.00	2021/11/19	Dan Zetzl	الإصدار الأول بعد تضمين تعليقات المراجعة.
01.01	2022/3/23	Dan Zetzl	تم تحديث عناوين URL في الجدول 2 لوجود خطأ إملائي في عنوان إنترنت الأشياء (IoT) وإدخال https لـ Radio Central.
01.02	2023/1/25		تمت إضافة اللغة الروسية.

الجدول 1: المراجعة السابقة للمستند

المراجع

[1] مخطِّط نظام إدارة الراديو، MN004686A01

[2] تعطيل التخزين المؤقت من جانب عميل DNS،
https://docs.microsoft.com/en-us/windows-server/networking/dns/troubleshoot/disable-dns-client-side-caching

مقدمة

تتطلب أجهزة MOTOTRBO Ion وR7 تنشيطًا مرة واحدة لتمكين ميزات البرنامج والخدمات التي تم شراؤها مع الجهاز.

لتبسيط التنشيط مرة واحدة ودعم الأجهزة غير المزودة بشاشة، يتم شحن أجهزة MOTOTRBO بملف تعريف افتراضي لشبكة Wi-Fi. وبالإضافة إلى تنشيط أجهزة MOTOTRBO مرة واحدة، يمكن للعملاء الذين يستخدمون تطبيق إدارة الراديو أو Radio Central اختيار استخدام شبكة Wi-Fi نفسها لتسجيل الجهاز في هذه التطبيقات من دون لمس.

يقدم هذا المستند توصيات حول أفضل الممارسات المرتبطة بأمان شبكة Wi-Fi المستخدمة للتنشيط مرة واحدة وتشغيلها.

توصيات حول أفضل الممارسات لشبكة Wi-Fi

تعيين عنوان IP

يتم تكوين أجهزة MOTOTRBO بشكل افتراضي لتحصل على عنوان IP عبر DHCP. ويتم تقديم التوصيات الآتية لضمان عدم نفاد تجمع عناوين IP المستخدم من قِبل خدمة DHCP في أثناء البرمجة المجمّعة للأجهزة.

1. يُوصى بتكوين خادم DHCP لاستخدام أوقات إيجار DHCP قصيرة. ويسمح لك ذلك بإعادة استخدام عناوين IP نفسها مع اكتمال مجموعات من أجهزة الراديو.
2. يُوصى بتكوين خادم DHCP ليشمل عددًا كافيًا من عناوين IP من أجل توفير عناوين لعدد أجهزة MOTOTRBO التي ستقوم ببرمجتها في الوقت نفسه في أثناء التوفير المجمّع، بالإضافة إلى الأجهزة الأخرى التي ستكون على الشبكة مثل مبرمج أجهزة إدارة الراديو. ملحوظة: يجب أن تأخذ في الحسبان وقت انتهاء مدة إيجار DHCP التي تمت مناقشتها أعلاه، وذلك ليسمح لك بإعادة استخدام عناوين IP تلك.

اكتشاف أجهزة MOTOTRBO (إدارة الراديو)

يتم تكوين أجهزة MOTOTRBO بشكل افتراضي لإرسال رسالة mDNS-SD[1] عند الاتصال بشبكة Wi-Fi وكل 90 ثانية بعد ذلك. ويرسل مبرمج أجهزة إدارة الراديو أيضًا رسائل mDNS-SD. يتم تقديم التوصيات الآتية لتمكين برنامج إدارة الراديو من اكتشاف أجهزة MOTOTRBO وقراءتها تلقائيًا من دون أي إجراءات مطلوبة من المستخدم.

1. رقم منفذ بروتوكول بيانات المستخدم (UDP) لـ DNS-SD هو 5353. عنوان IPv4 هو 224.0.0.251. ويجب أن تسمح قواعد جدار حماية الشبكة برقم المنفذ والبث هذين لكي تعمل الخدمة.
2. يجب أن يكون جهاز MOTOTRBO ومبرمج أجهزة إدارة الراديو موجودَين على مقطع الشبكة نفسه أو يجب إعادة توجيه حركة مرور الإرسال المتعدد بين مقاطع الشبكة (على سبيل المثال، باستخدام VLAN[2]). ويمكن عادةً العثور على تفاصيل حول كيفية تكوين معدات الشبكة لإعادة توجيه حركة مرور الإرسال المتعدد في كتيبات المنتج التي تخص الجهة المصنّعة لمعدات الشبكة.

[1] خدمة اسم مجال الإرسال المتعدد - اكتشاف الخدمة
[2] شبكة المنطقة المحلية الظاهرية

ملحوظة: يمكن تحديث وجهة اكتشاف الخدمة إلى عنوان IP أو اسم مضيف أحادي البث باستخدام برنامج إدارة الراديو.

تُرجى مراجعة مخطّط نظام إدارة الراديو للحصول على مزيد من التفاصيل.

توافر خادم وقت الشبكة

يتم تكوين أجهزة MOTOTRBO بشكل افتراضي لتحصل على الوقت الحالي عبر NTP[3].

خادم NPT الأوّلي	pool.ntp.org
خادم NTP الثانوي	time.google.com

تتطلب أجهزة MOTOTRBO التي تقوم بالتسجيل للشهادات باستخدام SCEP[4] وقتًا دقيقًا كجزء من CSR[5]. ويلزم توافر وقت دقيق للحصول على اتصال موثوق به بخدمة سحابة Radio Central.

استخدام قناة Wi-Fi

تدعم كل أجهزة MOTOTRBO تقنية Wi-Fi من الجيل 1 ((802.11b، وWi-Fi من الجيل 3 (802.11g)، وWi-Fi من الجيل 4 (802.11n).

ويدعم جهازا MOTOTRBO Ion وMOTOTRBO R7 أيضًا تقنية Wi-Fi من الجيل 5 (802.11ac) ويدعم MOTOTRBO Ion كذلك تقنية Wi-Fi من الجيل 6 (802.11ax).

يُعَد تحديد قنوات Wi-Fi غير متداخلة للوصول إلى أقصى حد من معدل النقل على الشبكة أحد أفضل الممارسات. وتنطبق هذه التوصية بشكل خاص على نقاط الوصول إلى Wi-Fi ذات التغطية المتداخلة، حيث يؤدي ذلك إلى تجنب تداخل القنوات المتجاورة بين نقاط الوصول إلى Wi-Fi.

في طيف التردد 2,4 جيجاهرتز، يُوصى بتحديد القنوات 1 و6 و11 لنقاط الوصول إلى Wi-Fi ذات التغطية المتداخلة. ملحوظة: قد تتداخل مصادر التشويش الأخرى، مثل أفران الميكروويف، مع أداء الشبكة.

[3] بروتوكول وقت الشبكة
[4] البروتوكول البسيط لتسجيل الشهادة
[5] طلب توقيع شهادة

في طيف تردد 5 جيجاهرتز، توجد 24 قناة غير متداخلة (36 و40 و44 و48 و52 و56 و60 و64 و100 و104 و108 و112 و116 و120 و124 و128 و132 و136 و140 و144 و149 و153 و157 و161 و165). بالإضافة إلى ذلك، توجد مصادر تشويش أقل. وستقوم بعض نقاط الوصول إلى Wi-Fi "بتوجيه" الأجهزة إلى تردد 5 جيجاهرتز بشكل افتراضي عن طريق إبطاء الاستجابات إلى تردد 2,4 جيجاهرتز.

يجب أخذ استخدام نقاط وصول متعددة لزيادة إجمالي النطاق الترددي المتوفر في الحسبان عند التوفير المجمّع.

توصيات حول أفضل الممارسات للأمان

يُعَد استخدام شبكة تسجيل لفصل العملاء غير الموثوق بهم عن شبكة الشركة من أفضل الممارسات الموصى بها. وفي حالة أجهزة MOTOTRBO، يتم تمكين شبكة التسجيل الأولية بشكل افتراضي.

معرف SSID الخاص بالمفتاح الذي تمت مشاركته سابقًا (PSK) لشبكة Wi-Fi الشخصية - MOTOTRBO
عبارة المرور: إدارة الراديو

تقييد الوصول المادي إلى شبكة التسجيل

يُعَد قصر الوصول المادي إلى منطقة تغطية Wi-Fi لشبكة التسجيل على الأفراد الموثوق بهم أحد أفضل الممارسات الموصى بها.

تغيير الإعدادات الافتراضية لشبكة Wi-Fi

يُعَد تحديث شبكة Wi-Fi وعبارة المرور إلى قيمة مغايرة للقيمة الافتراضية أحد أفضل الممارسات الموصى بها.

شبكات Wi-Fi للمؤسسات

من منظور أمني، يوفر استخدام شبكات Wi-Fi للمؤسسات مزايا متعددة عند مقارنتها بشبكات Wi-Fi الشخصية. وتتضمن المزايا القدرة على تعطيل الوصول إلى الشبكة على أساس جهاز فردي من دون التأثير في الأجهزة الأخرى الموجودة على الشبكة، وأن حركة المرور مشفرة بشكل فريد بين نقطة الوصول إلى Wi-Fi وكل جهاز، والقدرة على تحديث بيانات الاعتماد المستخدمة للتشفير بواسطة الممارسات القياسية لإدارة الشهادات. وتدعم أجهزة MOTOTRBO شبكات Wi-Fi الشخصية وشبكات Wi-Fi للمؤسسات.

استخدام قائمة التحكم في الوصول

يمكن استخدام قائمة تحكم في الوصول (ACL) لتقييد العملاء بشبكة التسجيل والخوادم والخدمات المطلوبة لتنشيط الجهاز فقط.

التطبيق أو الخدمة	اسم المضيف	المنفذ	الاتجاه	البروتوكول
NTP	Pool.ntp.org time.google.com	123	صادر	UDP
DHCP	غير منطبق (يتوفر بواسطة الشبكة)	67 68	صادر وارد	UDP
DNS	غير منطبق (يتوفر بواسطة الشبكة)	53	صادر	UDP و TCP
إدارة الشهادات	https://devicecertmgmt-cmf21.motsolpki.com https://devicecertmgmt-cmf21.motsolpki.com	49682 49684	صادر	https
Radio Central	locator.radiocentral.motorolasolutions.com	443	صادر	https
Radio Central	Api-us.radiocentral.motorolasolutions.com Api-au.radiocentral.motorolasolutions.com	443	صادر	https
Radio Central	Usp9rmstorage.blob.core.windows.net aup9rmstorage.blob.core.windows.net	443	صادر	https
خدمة إنترنت الأشياء	global.azure-devices-provisioning.net	443	صادر	https
خدمة إنترنت الأشياء	iotcs-hub-us.azure-devices.net	8883	صادر وارد	MQTT

الجدول 2: اتصالات شبكة الجهاز للتنشيط مرة واحدة