



OPEN CONNECT

## Netflix Open Connect Deployment Guide

This guide describes the deployment of embedded Open Connect Appliances. If you are interested in peering or an overview of the Open Connect program, see the [Open Connect web site](#).

**Last Updated:** 28 October 2024

*Copyright © 2024 by Netflix, Inc. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system, without express permission from Netflix, Inc*

Article is closed for comments.



OPEN CONNECT

## Requirements for deploying embedded appliances

The overall goal of Open Connect Appliance (OCA) deployment is to provide the best experience possible for Netflix viewers with a design providing maximum resiliency and localizing traffic as much as possible to optimize ISP resources. The following criteria have led to successful OCA deployments at a substantial number of global ISPs and are requirements for consideration.

### NETWORK AND DATA CENTER CRITERIA

Criteria	Description
Network	Your ISP should have a <b>public</b> autonomous system number (ASN) that you are able to use for peering
Netflix Viewer Traffic	For offload efficiency and system scale, we evaluate the level of current Netflix traffic to determine whether embedded OCA(s) can provide sufficient offload
Network Capacity	Each site must have the capacity to handle <b>1.2 Gbps of inbound traffic daily</b> per appliance for <b>fill and updates</b> . The majority of fill occurs during low traffic times to maximize offload.
Interconnection	You must connect to Netflix via SFI (peering) at one or more Netflix <b>points of presence (PoPs)</b> if it is possible to do so.
AWS Connectivity	OCAs and clients must be able to communicate with the control plane services running in Amazon Web Services (AWS). If connectivity to AWS is lost, OCAs will stop serving traffic. <b>Note:</b> You can confirm the status of required inbound/outbound OCA connectivity <b>in the Partner Portal</b> .
Installation	You must be able to <b>physically install</b> OCAs at your assigned site within <b>10 business days of receipt</b> , or as soon as possible thereafter
Consistent room temperatures	No higher than <b>78°F (26°C)</b>
Maximum room temperatures	No higher than <b>104°F (40°C)</b> for very short periods of time only

Physical Connection	You must be able to provision <b>1-2 X 100G or 2-6 x 10 Gbps optical ethernet ports in a LACP LAG</b> per OCA. The exact quantity depends on the OCA hardware type.
Maximum Power Supply Draw	350-700W per OCA, varies by hardware type and utilization

## TEAM ROLES

To participate in the OCA program, you will need to identify a person or a set of people who are available to perform the following roles. Your team members will work closely with the corresponding members of the Netflix team to facilitate the overall process.

Partner Role	Description
Engagement Manager	The main point of contact for the Netflix Open Connect team
Legal Representative	Reviews and accepts the legal agreements that are required for OCA deployments
Network Engineer	Provides information about partner sites, OCA configurations, maintenance, and network routing
Logistics Representative	Directs the shipment of OCAs  Your logistics representative should be involved at the beginning of the engagement process to avoid shipping delays at later stages of the process
Data Center Operations	Installs OCAs on the partner network
Network Operations	Works with Netflix to troubleshoot routing and other configuration issues that might arise

## TRAFFIC ANALYSIS AND SIZING

After Netflix receives your **OCA request**, we will review Netflix traffic patterns on your ASN. In general you will receive a response within 10 business days from submitting your request.

For ISPs who have one or more sites that qualify, additional capacity planning activities will be initiated. The first steps are to forecast per-site capacity and network configuration requirements in conjunction with your network planning and engineering teams. This includes analysis of traffic patterns within the various regions of your network, determination of the appropriate type and count of OCAs for each location, and a review of resiliency options.

The number of appliances to be deployed are determined by three general factors:

- Your overall network architecture requirements
- The peak Netflix traffic to be delivered from a given site
- The availability and failover options possible for a given site

Once appliances are deployed, the Netflix team will work with you to forecast future demand to ensure that your OCA configuration will accommodate future peaks of traffic. Appliance performance is monitored by the Open Connect Operations Team who will contact you if there are any issues with performance or the hardware itself. Note that per the Partner Maintenance section of the **Open Connect Deployment Guide** the only field-serviceable components are optics and power supplies. Any other hardware needs are met through our RMA process as described in the **Returns and Replacements** section of the guide.

Article is closed for comments.



OPEN CONNECT

## Requerimientos para la implementación de dispositivos OCA

English version: [Requirements for deploying embedded appliances](#)

El objetivo de la implementación de dispositivos Open Connect (OCA, Open Connect Appliance) es brindar la mejor experiencia posible a nuestros usuarios a través de un diseño que brinda la máxima resiliencia y localización de tráfico, optimizando los recursos del ISP. Los criterios a continuación son indispensables para la implementación exitosa de un OCA.

### CRITERIOS DE LA RED Y CENTRO DE DATOS

Criterio	Descripción
Red	Su ISP debe contar con un número de sistema autónomo (ASN) <b>público</b> que pueda ser usado para peering.
Tráfico de Netflix	Para lograr eficiencia en la descarga y escalabilidad del sistema evaluamos el nivel actual de tráfico de Netflix para determinar si el OCA/OCAs pueden proporcionar suficiente capacidad para atender la demanda.
Capacidad de la Red	Cada sitio debe tener la capacidad de atender <b>1.2 Gbps de tráfico entrante diario</b> por dispositivo para el <b>proceso de llenado y actualizaciones</b> . El periodo de llenado ocurre durante las horas de poco tráfico para maximizar la descarga.
Interconexión	Sugerimos conectarse con Netflix vía SFI(peering) en uno(s) de nuestros <b>puntos de presencia</b> (PoPs).
Conectividad a AWS	Los OCAs y clientes deben comunicarse con nuestro plano de control que opera en Amazon Web Services (AWS). Si la conectividad con AWS se pierde, los OCAs dejarán de servir tráfico.

**Nota:** Puede confirmar el status de conectividad entrante y saliente en el Portal de Socios ([Partner Portal](#)).

Instalación	El OCA deberá ser <b>instalado</b> dentro de un periodo de <b>10 días posterior a la entrega del dispositivo</b> , o tan pronto como sea posible a partir de entonces.
Temperatura ambiente constante	No superior a <b>78°F (26°C)</b>
Temperatura ambiente máxima.	No superior a <b>104°F (40°C)</b> por periodos de tiempo muy cortos
Conección Física	Debe contar con disponibilidad de <b>1-2 x 100G o 2-6 x 100G</b> puertos de Ethernet en LACP LAG. La cantidad exacta de puertos depende del tipo de hardware que reciba.
Consumo Máximo de Energía	350-700W por OCA, varía según el tipo de hardware y utilización.

## ROLES DEL EQUIPO

Para participar en el programa de Open Connect, debe identificar a una persona o grupo de personas que puedan cumplir con los siguientes roles. Los miembros de su equipo trabajarán de cerca con el equipo de Netflix durante el proceso.

Roles del Socio	Descripción
Project Manager	El punto de contacto principal para el Partner Engagement Manager (PEM) de Netflix.

Representante Legal	Revisa y acepta los acuerdos legales requeridos para la implementación del OCA(s).
Ingeniero de Red	Provee información sobre la localidad del despliegue, la configuración del OCA, mantenimiento, y enrutamiento.
Representante de Logística	Dirige la logística de recepción de los OCAs Su representante de logística debe estar envuelto desde el inicio del proceso para evitar retrasos en el proceso..
Operaciones de Centro de Datos	Instala los OCAs en la red/instalaciones del socio.
Operaciones de Red	Trabaja con Netflix para solucionar asuntos de enrutamiento, configuración y otros puntos que puedan surgir.

## ANALISIS DE TRAFICO

Una vez que Netflix recibe su **solicitud** de análisis de tráfico para participar del programa Open Connect, nuestro equipo revisa los patrones de tráfico de Netflix en su ASN. Recibirá una respuesta dentro de los 10 días hábiles posteriores a su solicitud.

Para aquellos ISPs que califiquen para el despliegue de OCAs en uno o más sitios, se iniciará el proceso de planificación de capacidad. El primer paso es pronosticar la capacidad por sitio y los requisitos de la configuración de su red, esto se lleva a cabo en conjunto con su equipo de planificación e ingeniería. El proceso incluye el análisis de los patrones de tráfico dentro de su red, la determinación del número y tipo de OCAs para cada sitio, y una revisión de las opciones disponibles de resiliencia.

El número de dispositivos que se implementarán está determinado por tres factores:

- Los requisitos generales de la arquitectura de su red
- El tráfico pico de Netflix que será entregado en un sitio determinado
- La disponibilidad y opciones de resiliencia de conmutación por error (failover) para un sitio determinado

Una vez que los dispositivos han sido implementados, el equipo de Netflix trabajará con usted para pronosticar la demanda futura y garantizar que sus OCAs puedan acomodar los picos de tráfico.. El desempeño del dispositivo es monitoreado por el equipo de Operaciones de Open Connect. En caso se

registre algún problema con el OCA en sí o con su desempeño, nuestro equipo lo contactará. Tenga en cuenta que, como se indica en la sección de Mantenimiento en la **Guía de implementación para Socios**, los únicos componentes que se pueden reparar son las ópticas y las fuentes de poder. Cualquier otra necesidad de hardware se completará a través de nuestro proceso de RMA, tal como se describe en la sección **Devoluciones y Reemplazos** de la misma guía.

Article is closed for comments.



OPEN CONNECT

## Summary of the embedded OCA deployment workflow

This article summarizes what partners can expect during the deployment process for embedded OCAs.

**Note:** With the exception of [Partner Portal invitations](#), all of the email correspondence related to OCA deployments comes from the following email alias: [info@partner.netflix.com](mailto:info@partner.netflix.com). You can also see these emails in the Partner Portal. For more information, see: [Viewing email communication in the portal](#)

The deployment workflow starts after you and one of our Open Connect team members have agreed that one or more OCAs will be sent to you. This workflow fits into our overall engagement workflow as described on the website in Step 5 (site survey) : <https://openconnect.netflix.com/en/#how-to-get-started>

- Site Survey (new or RMA)
- Partner Portal invitations
- Shipping Details
- Allocation, pre-fill, and network configuration
- Shipping / Receiving / Installing OCAs
- Turn-up / Burn-in
- Live / Monitoring

### SITE SURVEY (NEW OR RMA)

A *site survey* is a form that Netflix Open Connect uses to collect the information that we need in order to configure and ship OCAs to our partners. For new OCAs, your PEM or Service Manager will initiate a site survey. For RMAs, our Operations team will typically initiate a site survey. In either case, your identified contact will receive an email with a link to our [Partner Forms application](#), where your team will fill out shipping, contacts, and network configuration details.

For existing partners with Partner Portal access, you can also see and link to open or completed forms from the **Inbox** menu in the Partner Portal.

For more details on the site survey process, view the following video:



## PARTNER PORTAL INVITATIONS AND INFORMATION

After you complete and submit the site survey form, any new Engineering or NOC contacts that you identified in the form are invited to the Open Connect Partner Portal. An invite email is sent out with a link and instructions for how to active your portal account.

**Note:** Portal invitations come from a different alias. For information about the Partner Portal invitation process, see: [I am a brand new partner, how do I get portal access?](#)

If you are a brand new partner, this is a good opportunity to [add additional portal users](#) as needed.

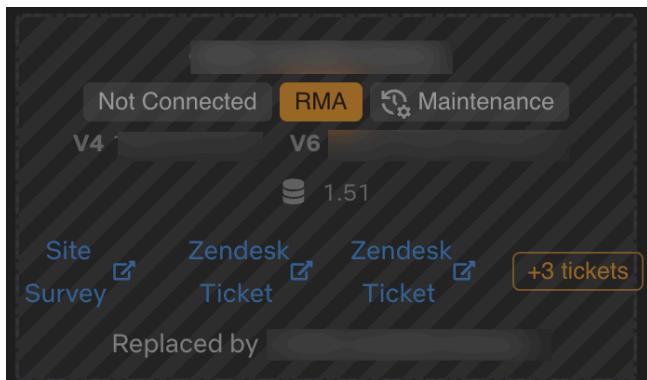
For more information about what you can do in the Partner Portal, see the [related articles](#) in this help center.

From the home page on the Partner Portal, you can view **Open Deployments** and their high level status from the home page. Click **Show More Deployments** to see additional details and links.

Site	Status	Type	Progress	Ticket	Forn
[REDACTED]	Delivered	Augment	●-●-●-●-	S	
[REDACTED]	Delivered	Augment	●-●-●-●-	S	
[REDACTED]	Delivered	Augment	●-●-●-●-	S	

Show More Deployments →

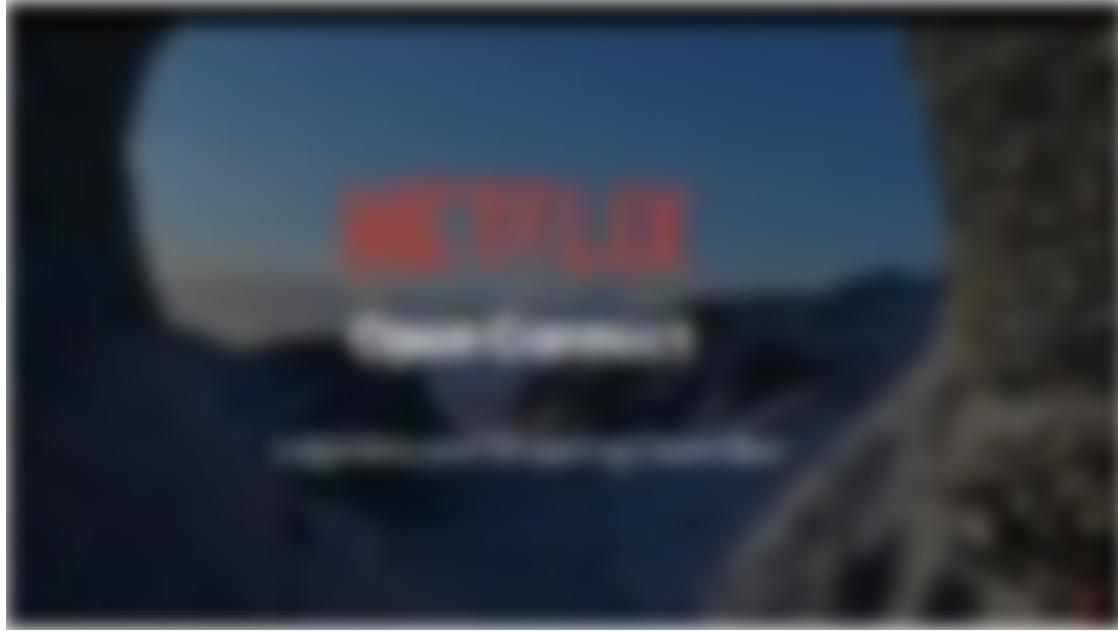
You can also discover OCAs that are in the process of being shipped and deployed, or OCAs that are flagged for RMA, from the **Embedded Sites** grid. For example:



## SHIPPING DETAILS

After you submit the site survey form, shipping details are finalized by the Open Connect logistics team in coordination with the shipping (and optionally, customs) contact that you identified in the site survey. After shipping details are agreed on and any necessary customs and import paperwork has been generated and approved, the shipping preparation process begins.

For more information about the logistics process, view the following video:

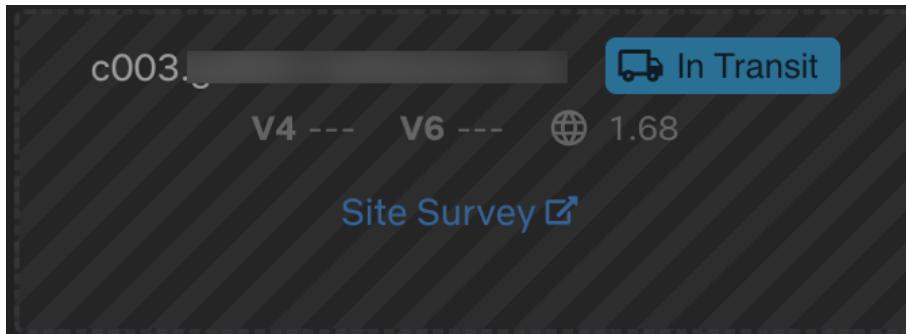


## PREPARING FOR SHIPPING

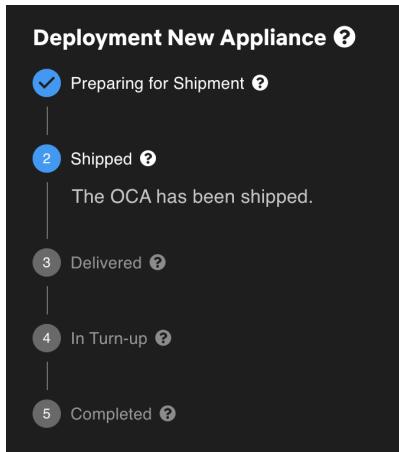
Contacts identified in the site survey receive an email when the shipping preparation process starts. Based on the hardware requirements for the deployment, we allocate specific hardware to your deployment and begin the process of pre-filling the OCAs with the appropriate catalog for your region. When the OCAs are done filling with content, we ship them to you.

## SHIPPING / RECEIVING

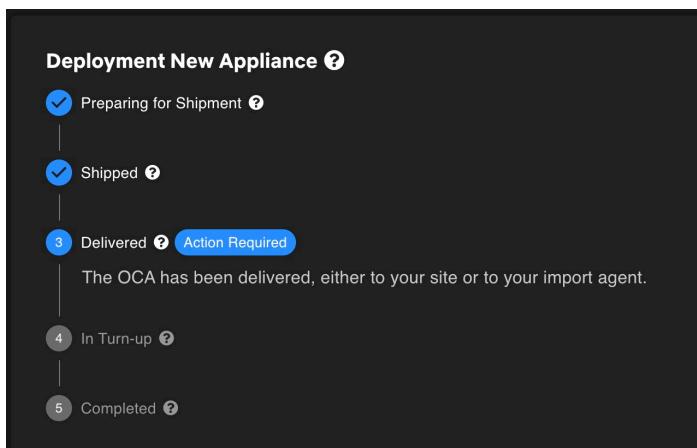
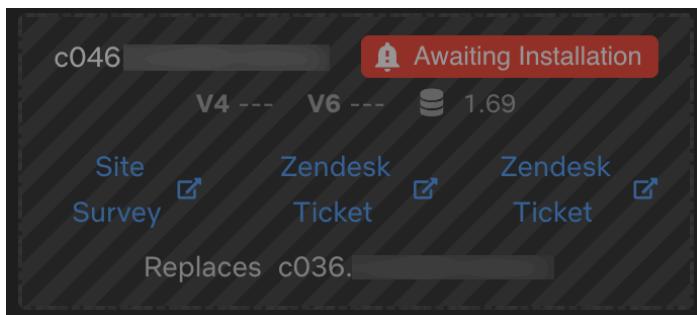
Contacts in the site survey receive an email when OCAs have shipped. A tracking number is provided in the email. During the shipping process, your OCAs are displayed in the Partner Portal on the home page or the site details page in an **In Transit** state.



On the OCA details page, a tracking diagram also reflects the current state of the shipment.



After OCAs are delivered to you, site survey contacts will receive another email letting you know. The Partner Portal homepage and the OCA details page will indicate that the OCAs are delivered and **Awaiting Installation**.



**Important:** You should physically install OCAs as soon as possible after delivery. This avoids having the pre-filled content become stale, requiring a lengthy on-site fill cycle before OCAs can begin to serve client traffic. This fill cycle can be costly if a large amount of content must be downloaded to the OCAs from distant sources.

For more details about the shipping and receiving process, see [the Shipping and Receiving section](#) in the Deployment Guide.

## INSTALLING OCAS AND ESTABLISHING BGP SESSION(S)

After OCAs are installed, connected to the internet, and a BGP session has been established with the appliance, they will begin to report health metrics and received routes to our control plane services. At this point, our systems are triggered to automatically begin the burn-in process.

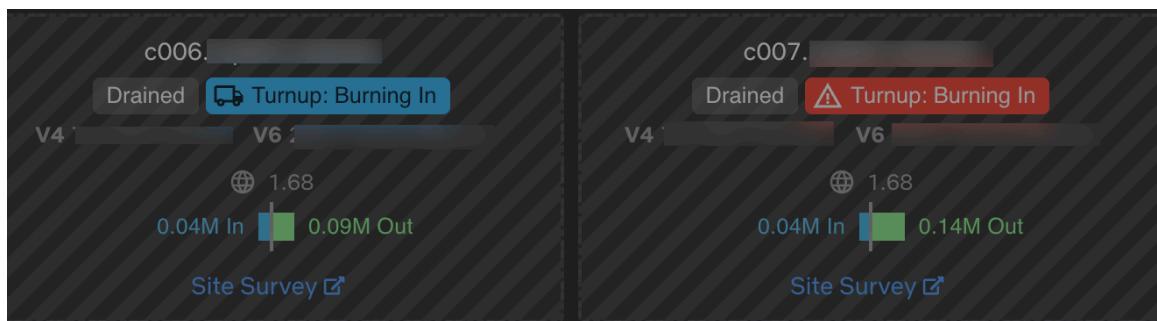
For more information about the installation process, see [Racking and Physical Installation of OCAs](#).

## BURN-IN AND TURN-UP CHECKS

You will receive an email when the burn-in process starts. During this process, the OCA will begin to receive fill traffic to bring the content catalog up to date. Assuming that the appliance was installed within a **reasonable amount of time** after receipt, the fill process generally takes **about two days**. If installation was delayed, the fill process can take longer.

In parallel, multiple status and health **turn-up checks** are periodically run on the appliance. You will receive emails with the results of each check and information about how to fix any failed checks.

The Partner Portal homepage and the Overview section of the OCA details page will indicate that the OCA is in turn-up. If any checks are failing, the OCA details page will indicate the errors and the Partner Portal homepage will indicate an Action Required state.



The screenshot shows the Netflix Open Connect Partner Help Center interface. At the top, there's a summary of a problem: "Network InErrors detected on TENO. Try cleaning or replacing the fi..." with a timestamp of "Failed at 2022-09-02 12:08:22, Next check at 2022-09-02 14:08:22". Below this, there are navigation links: Tickets (1), Audit Log, and Forms. The main content area is titled "Deployment New Appliance" and shows a checklist of steps: Preparing for Shipment (Completed), Shipped (Completed), Delivered (Completed), and In Turn-up (Action Required). A note states: "The OCA is in the process of being turned up to serve traffic. This process typically takes approximately 2 days after all checks pass." It also mentions "20/21 checks passing".

**Reminder:** You can also view details about passing/failing turn-up checks and other emails on the **Emails** page in the Partner Portal. For more information about turn-up checks and how to troubleshoot and fix them, see [this related article](#).

Appliances will not start serving client traffic until all checks pass and acceptable offload can be achieved. When the system is ready, the appliance is automatically enabled to serve clients and you will receive an email indicating that the OCA is live. At this point, the status for the OCA in Partner Portal will also switch to "Live". The Open Connect Operations team will then continue to monitor its performance.

For more information about the burn-in and turn-up process, view the following video:



## LIVE / MONITORING

The Open Connect Operations team constantly monitors OCA status and performance via our internal alerting and monitoring tools. Periodic software upgrades will automatically occur. These upgrades are timed to avoid peak traffic hours and typically do not require any action on your part. Engineering and NOC contacts in your organization will be notified via email when they start, and again when they finish. If any issues ever occur that require partner assistance, a ticket will be opened and your **Engineering** and **NOC** contacts will be notified about the ticket via email.

For more information about the checks that we run on Live OCAs, see this article: [OCA Live checks](#)

**Reminder:** If you need to power down an OCA in order to perform maintenance, you should disable it beforehand to gracefully **drain it of any live traffic** using the Partner Portal. Following this process will minimize any customer impact.

If you require assistance of any kind throughout this process or afterwards, [open a ticket](#).

Article is closed for comments.



OPEN CONNECT

## Shipping and Receiving OCAs

Netflix's logistics suppliers have different requirements for shipping, importing, and customs processes that are specific to each country in which your ISP operates. During the engagement process with Netflix, the shipping specifics for your country and deployment will be reviewed with you and agreed upon. You will be asked to confirm site readiness before any OCAs are shipped to you.

### SHIPPING OCAS

To facilitate smooth delivery and installation, you will be directed to an online site survey form before shipment where you can specify the configuration details of your appliances. In this form, you will provide information such as:

- Site physical address
- Shipping address
- Shipment contacts
- IP configuration details (IPv4, IPv6, default gateway, and so on)
- BGP configuration details (IPv4, and IPv6 if applicable)
- Type of rack rails (2-post vs 4-post)
- Power supply types (AC vs DC)
- Optic types

Before shipping OCAs to your facility, the Netflix team pre-configures the appliances and fills them with the latest content. To avoid having the pre-filled content become stale, thereby requiring an extended high-traffic initial fill period, it is highly recommended to get the appliances online as soon as possible.

Each appliance is shipped with the appropriate parts, based on what you specify in the online form.

### RECEIVING OCAS

Requirements for receiving an appliance shipment are roughly as follows. Specific requirements will be communicated to your logistics team by the Netflix logistics team before the shipment.

Criteria	Requirement
Estimated appliance weight	<b>100 to 125 pounds (45 to 57 kg)</b>
Estimated weight of pallet and shipping materials	<b>63 pounds (29 kg)</b>

## Loading dock and jack

Upon request, Netflix will ensure delivery trucks arrive with a pallet jack and lift gate if a loading dock and jack are not available at the destination.

---

Article is closed for comments.



OPEN CONNECT

## Racking and Physical Installation of OCAs - PDF ONLY

FOR ADDITIONAL VIDEO INSTRUCTIONS ON HOW TO INSTALL YOUR OCA, PLEASE REFER TO:  
**RACKING AND PHYSICAL INSTALLATION OF OCAS**

- Overview
- Unboxing the OCA
- Racking the OCA
- Installing optic connectors and fiber cable
- Installing power supply units (PSUs)
- OCAs Defective on Receipt
- Next Steps

### OVERVIEW

Netflix ships each OCA to your requested location ready to deploy. As soon as you receive your OCA shipment, you are responsible for:

- Racking the appliance
- Providing the necessary 1-2 X 100G or 2-6 x 10Gbps optical network connections. Exact quantity depends on the appliance type.

**Reminder:** Because the content that is pre-loaded onto the appliances can become stale quickly, you should complete the installation as soon as possible.

### RACKING THE OCA

**Rack type:** OCAs are either 2- or 4-post rack friendly.

#### Airflow:

- Optics might face either the hot or the cold aisle.
- Airflow is marked on the OCA, and these markings should be taken as the source of truth. If you are unsure about what type of OCA you are installing or have a question about airflow, [open a ticket](#).

#### Racking Guidelines:

- **Elevated Operating Ambient:** If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.
- **Reduced Air Flow:** Installation of the equipment in a rack should be such that the amount of airflow required for safe operation of the equipment is not compromised.

- **Mechanical Loading:** Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- **Circuit Overloading:** Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- **Reliable Earthing:** Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

Refer to these additional rail kit instructions:

#### OCA rail kit instructions

## INSTALLING OPTIC CONNECTORS AND FIBER CABLE

Install the optics connector(s) and fiber optic cable(s) that came with the OCA.

For Global OCAs only, we also include a copper connector that can be used to enable out-of-band access between a healthy OCA and an OCA that is offline. Storage and Flash OCAs have this type of connector integrated into the motherboard. On Global OCAs, the copper connector should come already inserted into the LAN1 port, and you will only need to connect it as needed for troubleshooting. For more information see: [Enabling out-of-band access to an offline OCA](#)

## INSTALLING POWER SUPPLY UNITS (PSU)

Install the power supply units (PSUs) that came with the OCA.

**DC Power:** If you are using DC power, follow these supplemental instructions:

#### DC Power Adapter instructions

After you have installed the PSU, connect the power cables and power on the OCA.

## OCAS DEFECTIVE ON RECEIPT

If an OCA is defective upon receipt, Netflix will send a Return Material Authorization (RMA) replacement appliance. For more information see: [Returns and replacements](#)

In the event of a hardware failure, please [open a ticket](#) for assistance.

## NEXT STEPS

After the initial installation, the next step is to establish a BGP session with the appliance, following the [network configuration instructions](#). After the session is established and the appliance begins reporting data, the OCA will begin to receive fill traffic and begin a burn-in cycle.

Assuming that the appliance was installed within a **reasonable amount of time** after receipt, the fill process generally takes about two days. If installation was delayed, the fill process can take longer.

During the burn-in period, multiple **turn-up checks** are run on the appliance. You will receive periodic emails with the results of the turn-up checks, and any failing checks are also visible in the Partner Portal with links to additional troubleshooting information. The appliance will start serving test client traffic after all checks pass and the OCA has filled with sufficient current content such that acceptable offload can be achieved. When the system is ready, the Netflix Open Connect operations team will transition the OCA to a Live state and will continue to monitor its performance.

- [dc-power-supply-adapter-kit.pdf](#) (300 KB)

Article is closed for comments.



OPEN CONNECT

## Network configuration

This article is also available in Brazilian Portuguese and Spanish:

- [Configuração de rede](#)
- [Configuración de la Red](#)

This section describes how Open Connect Appliances are typically configured in a network. If you are an Open Connect ISP partner, Netflix works closely with you to determine the optimal configuration for your particular needs.

For more information, see the [FAQs](#)

- [Overview](#)
- [Router interface configuration](#)
- [Reconfiguring the IP address of an OCA](#)
- [Routing and content steering via BGP advertisements](#)
- [Clustering architectures](#)
- [Flash-based appliances](#)

## OVERVIEW

OCAs are *directed cache appliances*, meaning that the manner in which traffic is directed to the appliance is determined explicitly by you and by Netflix, not by the appliance itself.

An OCA only serves clients at IP addresses that you advertise to the OCA via a BGP session. In other words, traffic is only delivered from your embedded OCAs to the customer prefixes that you explicitly announce to them, as described in the following sections. Therefore, you as the ISP partner have full control over the networks that the appliances will serve. BGP sessions are established between appliance(s) and the closest connected router.

If content is requested that is not contained on an embedded OCA, the client request is directed to the closest Netflix content site via peering (if present) or via transit.

## RECONFIGURING THE IP ADDRESS OF AN OCA

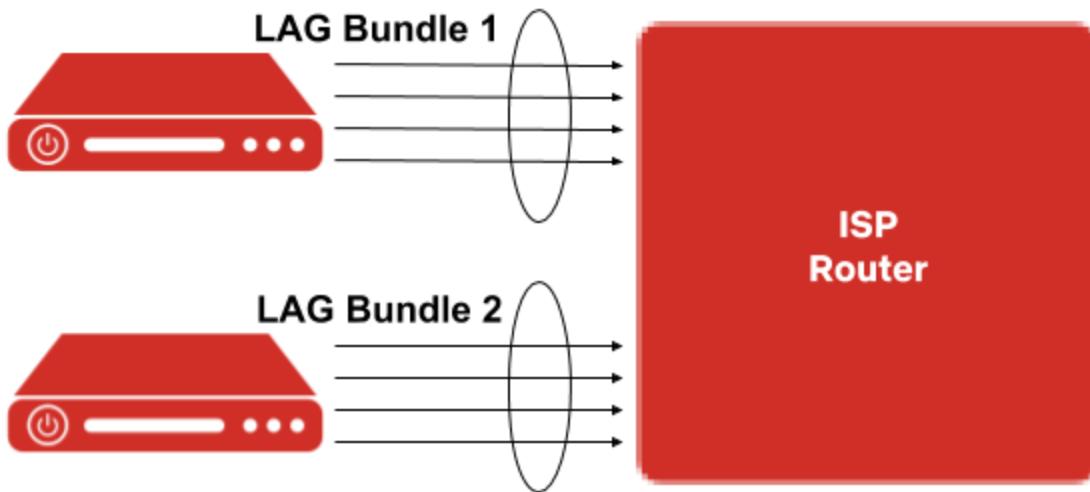
Each appliance comes fully configured based on the IP address details that you provided to Netflix in your site survey before it was shipped.

For step by step instructions on how to change the IP address of an OCA, see the following article: [Updating the IP address of an OCA](#)

## ROUTER INTERFACE CONFIGURATION

When you are connecting the appliances to your router, follow the guidelines in this section. See also [Example router configurations](#).

- Each OCA must be assigned one publicly routable IPV4 address, and it is highly recommended to also assign one IPV6 address.
- You can assign an address to the appliance from an IPv4 subnet of /31 and larger, or an IPv6 subnet of /127 and larger.
- It is acceptable to assign an address to the appliance from a larger subnet (for example, a /24). However, because only one IPv4 address is required per appliance, a smaller subnet is typically used.
- The router interfaces must be configured for Link Aggregation Group (LAG) with LACP. Each server must be configured in its own LAG bundle for the active interfaces on each server, as illustrated in the diagram below. In the two-server example configuration, there are two separate LAG bundles, one for each server.



- A standard maximum transmission unit (MTU) must be configured on each router interface. Jumbo frames are not supported.
- If there are multiple routers available that can provide redundancy in a site, it is recommended to stagger appliances between routers. Appliances on the same router should be in the same subnet to optimize filling. Appliances on separate routers should be in separate subnets. Appliances are not designed to be connected to two separate routers.
- All ports on an OCA must be connected to the same router or switch. Using multi-chassis LAG or switch stacking is not supported.
- Each OCA is hardened against network attacks and is designed to be directly connected to the internet. Filtering inbound or outbound traffic can cause operational issues, so we strongly recommend that you allow all traffic on all ports, do not use ACLs, and ensure that your router has a default route or full routing table. If you absolutely **must** filter, the current list of inbound and outbound usage follows. Please note that this list can change at any time without prior notification.
  - **Traffic from OCA:** Allow all destination addresses and ports.
  - **Traffic to OCA:** Allow TCP 22, 53, 80, 179, 443, UDP 53 and 123 (source and destination), ICMP types 0, 3, 8, 11, and all ICMPv6 from any public IP/port. Allow all return traffic from any appliance-initiated connection (TCP established).

- **Note:** You can confirm the status of required inbound/outbound OCA connectivity [in the Partner Portal](#).
- Each network interface must be receiving between 0 dBm and -10 dBm of light to ensure good data throughput. The LCD panel on the front of the appliance displays the current light levels for each interface. If your appliance does not have an LCD panel, [access the console](#) with a keyboard and mouse.
  - For more information see the following related articles:
    - [Checking optical signal strength on an OCA](#)
    - [Troubleshooting input errors or low light levels on an OCA](#)

## ROUTING AND CONTENT STEERING VIA BGP ADVERTISEMENTS

We steer clients to our OCAs based on an ISP's BGP advertisements, coupled with the routing and steering algorithms in the Open Connect control plane. ISP partners can control some aspects of content steering via the BGP routes that are announced via peering or to each embedded OCA.

The control plane steers clients to the best available OCAs using a modified version of BGP best path selection. Assuming that the appliance has the requested title and available serving capacity, the control plane provides clients with a ranked list of appliances (typically 3 or more reliable sources) to stream from.

### APPLIANCE SELECTION CRITERIA

The following appliance selection criteria are considered, in order, by the Open Connect control plane services. If there is a tie for a given criterion, then the next criterion is considered. If there is a tie on all criteria, traffic is balanced between appliances.

1. The appliance that receives the most-specific route to the client's prefix.
2. The appliance that receives the route to the client's netblock with the shortest AS path. (See the [notes on peering](#) below).
3. The appliance that receives the route to the client's netblock with the lowest multi-exit discriminator (MED). (See the [notes on MEDs](#) below).
4. The geographically closest appliance\*. We geolocate based on client IPs, whose location is then compared to the latitude and longitude of nearby OCAs to determine the closest available system.

**\*Note:** If you have two redundant embedded sites that are geographically well-connected, **and** they are designed to serve the same set of customers (with the same prefixes advertised to both sites), it is possible for Netflix to set a geo override so that traffic will be equally balanced across both sites. If you have this situation, you can [open a ticket](#) to request a geo override.

### ADDITIONAL NOTES ON MEDS

- We honor the MED values that we receive. However, we increase the value as follows depending on where we learn the prefix:
  - +0 for an embedded OCA (Netflix Cache server)
  - +50 for a direct peering connection (PNI)
  - +100 for peering at an IX (public peering)
- There is no cap on the maximum MED value.
- A missing MED is treated the same as a MED of 0, and indicates that the appliance should receive all servable traffic for the associated prefixes (also often referred to as *MED-missing-as-best*). Remember,

if multiple appliances receive the same prefix with the same metric, traffic is load-balanced across those appliances. Because a missing MED will be equivalent to 0, it is preferred over any >0 MED on other appliances.

- **Important:** Marking MEDs on already installed and working Open Connect Appliances can be hazardous, because it must be done on all BGP sessions for all appliances at the same time.

Finally, a reminder that if you are peering with Netflix and do IRR filtering, our prefix set is RS-NETFLIX and our as-set is AS-NFLX. Please be sure to accept advertisements that originate from ASNs: 2906, 40027, and 55095.

See also: [Peering Locations](#).

## BGP REQUIREMENTS

- Route announcements for Open Connect embedded appliances:
  - IPv4 prefixes between /8 and /31 (inclusive) are accepted.
  - IPv6 prefixes between /19 and /64 (inclusive) are accepted.
- Route announcements for Open Connect peering sessions:
  - IPv4 prefixes between /8 and /24 (inclusive) are accepted.
  - IPv6 prefixes between /19 and /48 (inclusive) are accepted.
- As an implicit requirement, **all** appliances must have a BGP session configured in order to correctly participate in Netflix content steering and delivery.
- To localize traffic, the best practice is to advertise the most specific routes to the appliance. For example, if you are announcing a /22 to the OCA, but a /24 is received from the same block over settlement-free interconnection (SFI) peering or transit, the /24 will be preferred, delivering content traffic from the remote source instead of the OCA.
- If you are deploying only one OCA in your network, you should advertise the most specific (longest) prefix for that OCA over the peering session that you want the OCA to use for nightly filling purposes.
- If you are deploying multiple OCAs across more than one site in your network:
  - To enable efficient nightly fill: ensure that the appliances within one site can hear the subnets for the appliances in the other site via the BGP connection that is established with your router. See the [Fill and updates](#) information for more details.
  - See the additional information about [clustering architectures](#).
- Netflix does not use any BGP community information that is advertised by partners to OCAs or via Open Connect peering.
- Advertised routes that are received by an OCA are synchronized with Open Connect control plane services approximately every five minutes.
- If you are planning to serve client traffic from your embedded OCAs to prefixes within an ASN that is outside of your network, ensure that you are [Documenting Network Relationships with an AS-SET](#)
- Netflix uses RPKI-based route filtering. For more information, see: [RPKI-based route filtering](#).
- Netflix has joined the MANRS initiative. For more information, see: [Mutually Agreed Norms for Routing Security \(MANRS\)](#)

## TROUBLESHOOTING BGP ADVERTISEMENTS

There are a few tools in the Partner Portal that you can use to explore and troubleshoot BGP announcements:

- Use the **Route Explorer** to monitor the state of the BGP sessions and announcements that you have configured between your routers and the Netflix Open Connect Appliances that are embedded in your network.
- Use the **Route Optimizer** to run reports on your BGP route announcements. The **Route Optimizer** reports include all announcements that Netflix hears from your ASN(s), including at peering and embedded sites.
- View the **Route Performance Report** to discover prefixes in your network that are potentially experiencing relatively poor video streaming quality.

## EMBEDDED OCAS COMBINED WITH PEERING SESSIONS

The ideal Open Connect implementation is a mixture of both SFI peering and deployed embedded OCAs. Netflix uses two separate autonomous systems for peering:

- AS2906 is the AS number that Netflix uses for peering at its PoPs
- AS40027 is the AS number that embedded OCAs use to peer with ISP networks

See **BGP requirements** for prefix announcements that are accepted on peering sessions.

When OCAs and Open Connect SFI peering is combined, peering is used primarily for backup, for filling, and for serving long-tail titles.

Assuming that the AS PATH LENGTH to an embedded OCA and peering are equal, if you announce the same prefix both to a private or public peering session (using AS2906) and to an OCA (using AS40027) the OCA will be preferred over peering. This is because the Open Connect control plane will have two BGP entries for that prefix:

- one with an AS PATH LENGTH of 1 (<AS\_NUMBER>) from the appliance itself
- one with an AS PATH LENGTH of 2 (2906 <AS\_NUMBER>) from the peering location

Keep in mind the **appliance selection criteria** above and remember that the general best practice is to announce more specific routes to embedded appliances so that they are preferred for serving traffic.

## CLUSTERING ARCHITECTURES

The number of OCAs deployed to each embedded site will depend on the volume of Netflix traffic being served from the site. In many cases, a single OCA is sufficient. However, if the volume of traffic warrants additional OCAs within a site, we configure them as a single manifest cluster. OCAs in a manifest cluster share content storage and function together as one logical server/storage unit.

Although partners do not need to configure manifest clusters, it is important to understand some basic clustering concepts. In particular, there are implications to consider when OCAs in a cluster are taken down for maintenance or moved to a different site.

Clustering the OCAs within a site allows for greater offload for unique content. In a two-OCA cluster, both appliances will use approximately 40% of their storage for the same popular content. This popular content typically represents roughly 60% of the OCA's total offload. The remaining 60% of storage space on each OCA is used to store a unique set of less-frequently-accessed content. Because we do not store the same exact set of content on each single OCA in a cluster, a cluster of OCAs provides greater total offload than an unclustered group of OCAs. This strategy helps the OCAs in a site function more efficiently.

For more information about storage strategies, see [this tech blog post](#).

## IMPORTANT NOTES FOR PARTNERS:

- After a set of OCAs has been installed in a site and grouped together as a cluster by the Open Connect team, they should be thought of as one big server. Therefore, any changes you make to a single OCA in a site has the potential to negatively impact the serving efficiency and behavior of the group.
- If you need to make changes to the OCAs in an established site - for example, if you intend to relocate an OCA from one site to another or disable one or more OCAs for a significant period of time - it is important to notify the Open Connect team so that they can make the necessary changes to the cluster configuration. Failing to do so can cause undesired consequences. For example, you may see traffic being steered to the wrong site, fill patterns may become suboptimal, and hot spots might develop.
- To enable optimal and balanced traffic patterns, OCAs in a site must receive the exact same BGP route advertisements. Therefore, if you relocate an OCA you must revisit your BGP route announcements to ensure that traffic continues to be steered appropriately.

## FLASH-BASED APPLIANCES

If you are an ISP with very large amounts of Netflix traffic, we may include flash-based appliances in your OCA deployment architecture. Flash-based appliances are flash memory-based servers that are deployed when you reach a threshold number of OCAs, to augment the delivery capability of the main (storage) appliances.

Article is closed for comments.



OPEN CONNECT

## Configuración de la Red

English version: [Network configuration](#)

Esta sección describe la configuración de los dispositivos Open Connect (OCA, Open Connect Appliance). Si usted es un proveedor de servicios de internet (ISP, Internet Service Provider) socio de Open Connect, Netflix trabajará con usted para determinar la configuración óptima en base a sus necesidades.

Para más información, visite la página de [Preguntas frecuentes](#).

### DESCRIPCIÓN GENERAL

Los OCAs son dispositivos dirigidos (directed cache appliances), esto quiere decir que la manera como el tráfico es dirigido al dispositivo es determinado por usted y Netflix, no por el dispositivo en sí.

Un OCA solo atiende a usuarios en las direcciones IP que usted anuncia hacia el, a través de una sesión BGP. El tráfico solo se entrega desde sus OCAs a los prefijos anunciados específicamente por usted. Por lo tanto, usted—como nuestro socio—tiene el control sobre la red atendida por los dispositivos. Las sesiones BGP son establecidas entre el dispositivo(s) y el router más cercano.

Si el contenido que solicita un usuario no se encuentra alojado en su OCA, el pedido se dirige al sitio de contenido de Netflix más cercano, ya sea vía un acuerdo de interconexión o peering (si está disponible) o vía tránsito.

### RE-CONFIGURACIÓN DE LA DIRECCIÓN IP EN UN OCA

Cada dispositivo viene completamente configurado con la información proporcionada por usted en el cuestionario de sitio.

El artículo, [Actualización de la dirección IP en un OCA](#), detalla paso a paso cómo cambiar la dirección IP en el dispositivo.

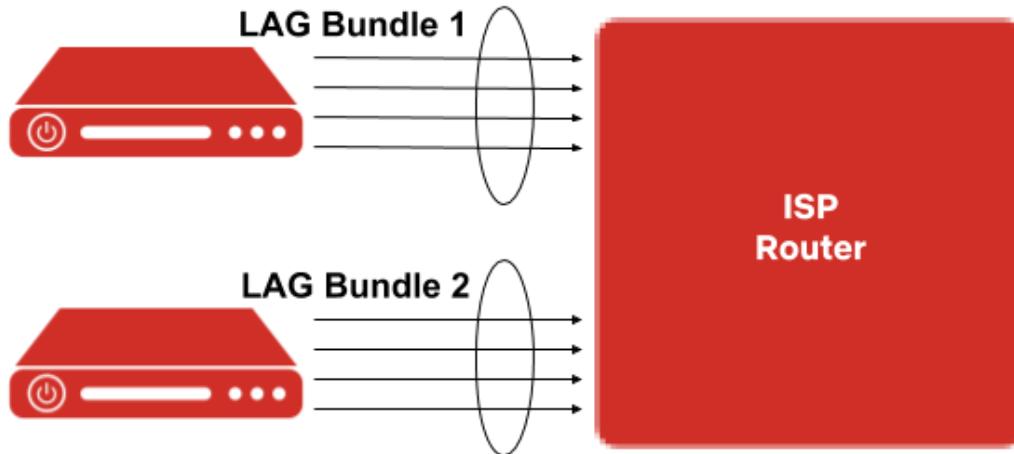
### CONFIGURACIÓN DE LAS INTERFACES DEL ROUTER

Cuando esté conectado el/ los dispositivo (s) OCAs a su router, siga esta sección. También puede ver el artículo, [Ejemplos de configuraciones de router](#).

- Cada OCA debe tener asignado una dirección IPv4 pública. Recomendamos también asignar una dirección IPv6.
- Usted puede asignar una dirección IPv4 de una subred /31 o mayor, o de una IPv6 /127 o mayor.
- Es aceptable asignar una dirección de una subred más grande (por ejemplo, /24). Sin embargo, como solamente se requiere una dirección IPv4 por dispositivo, normalmente se usa una subred más

pequeña

- Las interfaces del router deben ser configuradas en grupos de adición de enlaces (LAG Link Aggregation) con el protocolo de control de adición de enlaces LACP. Como se muestra en el siguiente diagrama, cada servidor debe ser configurado en su propio grupo LAG. En el caso de tener dos servidores, hay dos LAG diferentes, uno por cada servidor.



- Cada interfaz debe tener configurada la unidad máxima de transmisión estándar (MTU). Los *jumbo frames* no son compatibles.
- En caso haya múltiples routers disponibles en un sitio para proporcionar redundancia, se recomienda alternar los dispositivos entre routers. Los dispositivos conectados a un mismo router deben estar en la misma subred para optimizar el proceso de llenado. Los dispositivos conectados a routers separados deben estar en diferentes subredes. Los dispositivos no están diseñados para estar conectados a dos routers separados.
- Todos los puertos en el OCA deben estar conectados al mismo router o switch. No se recomienda *multi-chassis LAG* o *switch stacking*.
- Cada OCA está protegido contra ataques y está diseñado para ser conectado directamente al internet. Filtrar el tráfico de entrada o de salida, puede causar problemas operacionales, debido a eso recomendamos encarecidamente autorizar todo tipo de tráfico en todos los puertos, no usar ACLs, y asegurarse que su router tenga una ruta predeterminada o una tabla de enrutamiento completa. En caso usted requiera aplicar filtros, a continuación se presenta un lista de uso de salida y entrada. Por favor tenga en cuenta que esto puede cambiar en cualquier momento sin notificación previa.
  - Tráfico desde el OCA:** Permita todas las direcciones y puertos de destino
  - Tráfico hacia el OCA:** Permita TCP 22, 53, 80, 179, 443, UDP 53 y 123 (origen y destino), ICMP tipo 0, 3, 8, 11, y ICMPv6 desde cualquier IP/puerto público. Permita todo el tráfico de retorno desde cualquier conexión iniciada por el dispositivo (TCP establecido).
  - Nota:** En el [Portal de Socios](#) (Partner Portal) puede confirmar el status de conectividad entrante/saliente del dispositivo.
- Cada interfaz debe recibir entre 0 dBm y -10 dBm de luz para asegurar un buen flujo de datos. El panel LCD en la parte frontal del dispositivo muestra los niveles de luz de cada interfaz. Si su dispositivo no tiene un panel LCD, puede acceder a la consola con un teclado y mouse.
  - Puede encontrar más información en los siguientes artículos:
    - [Comprobar la intensidad de la señal óptica en el OCA](#)
    - [Soluciones a errores de entrada o niveles bajos de luz en el OCA](#)

## ENRUTAMIENTO Y DIRECCIONAMIENTO DEL CONTENIDO VÍA ANUNCIOS BGP

Nuestros usuarios son dirigidos hacia los OCAs en base a los anuncios BGP de un ISP, en conjunto con los algoritmos de enrutamiento y direccionamiento en el plano de control de Open Connect. Los socios pueden controlar algunos aspectos del direccionamiento del contenido a través de las rutas BGP anunciadas vía peering o a cada una de las OCAs integradas en su red.

El plano de control dirige a los usuarios al mejor OCA disponible utilizando una versión modificada de la selección de la mejor ruta de BGP. Asumiendo que el dispositivo posee el título solicitado y capacidad de servicio disponible, el plano de control provee a los usuarios una lista de los dispositivos (usualmente 3 o más fuentes confiables) de donde transmitir el contenido.

### CRITERIOS DE SELECCIÓN DE DISPOSITIVO

Los siguientes criterios de selección de dispositivo son considerados, en orden, por el plano de control de Open Connect. Si hay un empate por un criterio dado, se considera el siguiente criterio. Si hay un empate en todos los criterios, el tráfico se balancea entre los dispositivos.

1. El dispositivo que recibe la ruta más específica hacia el prefijo del usuario.
2. El dispositivo que recibe la ruta hacia el *netblock* (o rango de direcciones IP consecutivas) del usuario con la ruta AS más corta. (Ver abajo las notas sobre peering).
3. El dispositivo que recibe la ruta hacia el *netblock* del usuario con el MED más bajo (MED, multi-exit discriminator). (Ver Notas Adicionales acerca de MEDs)
4. El dispositivo ubicado geográficamente más cercano\*. La geolocalización se basa en el IP del usuario, cuya ubicación se compara con la latitud y longitud de los dispositivos cercanos para determinar el sistema disponible más cercano.

**\*Nota:** Si usted tiene dos sitios redundantes que están bien conectados, y están diseñados a servir el mismo grupo de clientes (con los mismos prefijos anunciados en ambos sitios), es posible para Netflix establecer un *geo override* (anular el criterio de geolocalización) de ese modo el tráfico se equilibra igualmente entre los dos sitios. Si usted cuenta con una situación como la descrita, puede abrir un ticket para pedir un *geo override*.

### NOTAS ADICIONALES ACERCA DE MEDS

- Los valores MED que recibimos se respetan. Sin embargo, los valores se incrementan dependiendo de donde están ubicados los prefijos:
  - +0 para un OCA (servidor de Netflix)
  - +50 para una conexión directa de peering (PNI)
  - +100 para peering en un IX (peering público)
- No hay límite para el valor máximo de MED.
- Un MED omitido es considerado como un MED con valor 0, lo cual indica que el dispositivo debería recibir todo el tráfico para los prefijos asociados (esto se refiere también como *MED-missing-as-best*). Recuerde, si varios dispositivos reciben el mismo prefijo con la misma métrica, el tráfico se equilibra en todos esos dispositivos. Debido a que un MED omitido equivale a 0, éste se prefiere en lugar de cualquier otro MED con valor >0 en otros dispositivos.
- **Importante:** Añadir MEDs en un OCA ya instalado y operativo puede causar problemas, ya que deben añadirse en todas las sesiones BGP en todos los dispositivos en un mismo sitio.

Por último, recuerde que si usted tiene un acuerdo de interconexión o peering con Netflix, y utiliza el filtrado IRR, nuestro prefix-set es RS-NETFLIX y nuestro as-set es AS-NFLX. Por favor asegúrese de aceptar anuncios que se originan desde ASNs: 2906, 40027, y 55095.

## REQUERIMIENTOS DE BGP

- Anuncios de enrutamiento para dispositivos Open Connect:
  - Se aceptan prefijos IPv4 entre /8 y /31 (inclusive).
  - Se aceptan prefijos IPv6 entre /19 y /64 (inclusive)
- Anuncios de enrutamiento para sesiones de peering Open Connect:
  - Se aceptan prefijos IPv4 entre /8 y /24 (inclusive).
  - Se aceptan prefijos IPv6 entre /19 y /48 (inclusive).
- Como requerimiento implícito, todos los dispositivos deben tener una sesión BGP configurada a fin de participar correctamente en el direccionamiento y entrega del contenido de Netflix.
- Para localizar tráfico, la mejor práctica es anunciar las rutas más específicas al dispositivo. Por ejemplo, si anuncia un /22 al OCA, pero un /24 es recibido a través de peering o tránsito, se prefiere el /24 al /22, y el contenido es entregado desde una fuente remota en lugar de ser entregado desde el OCA.
- Si solo está instalando un OCA en su red, el prefijo más específico (el más largo) debería ser anunciado en ese dispositivo durante la sesión de peering que desee usar para el llenado nocturno.
- Si está instalando múltiples OCAs es más de un sitio en su red:
  - Para permitir un llenado nocturno efectivo: asegúrese que los dispositivos ubicados en un sitio puedan escuchar las subredes de los dispositivos ubicados en otro sitio vía la sesión BGP establecida en su router. Para más información consulte el artículo [Patrón de llenado](#).
  - Más información disponible en la sección Arquitectura de Cluster.
- Netflix no usa la información de ninguna comunidad BGP anunciada por socios a los OCAs o vía peering Open Connect.
- Las rutas anunciadas que recibe un dispositivo se sincronizan con el plano de control de Open Connect aproximadamente cada 5 minutos.
- Si planea anunciar prefijos de otras redes/ASN en sus OCAs asegúrese de documentar la relación en su AS-SET. Para más información consulte el artículo, [Documentando la relación entre redes con un AS-SET](#).
- Netflix utiliza el filtrado RPKI. Para más información consulte el artículo [Filtrado RPKI en sesiones BGP](#).
- Netflix se ha unido a la iniciativa MANRS. Para más información consulte el artículo: [Normas Mutuamente Acordadas para los Estándares de Seguridad de Enrutamiento \(MANRS\)](#).

## RESOLUCIÓN DE PROBLEMAS DE ANUNCIOS BGP

El Portal de Socios cuenta con herramientas que pueden ayudar a explorar y ofrecer soluciones a problemas relacionados con anuncios de BGP.

- La herramienta [Route Explorer](#) monitorea el estado de las sesiones BGP y los anuncios configurados entre sus routers y sus OCAs.
- La herramienta [Route Optimizer](#) ejecuta reportes de sus anuncios BGP. Los reportes incluyen todos los anuncios que Netflix escucha desde su ASN(s), incluyendo los de las sesiones de peering y sitios con OCAS.

- La herramienta **Route Performance Report** muestra los prefijos de su red que posiblemente experimenten una baja calidad de transmisión de video.

## OCAS COMBINADO CON SESIONES DE PEERING

Al participar de Open Connect, lo ideal es contar con acuerdos de interconexión gratuitos o peering y OCAs. Netflix utiliza dos sistemas autónomos diferentes para hacer peering:

- AS2906 es el AS que Netflix utiliza para hacer peering en sus Puntos de Presencia.
- AS40027 es el AS que se usa para que los OCAs hagan peering con los ISPs.

En la sección Requerimientos de BGP puede ver los prefijos que se aceptan en las sesiones de peering.

Cuando se cuenta con ambos, OCAs y acuerdos de peering, la sesión de peering se usa principalmente como soporte o backup, para llenado, y para servir los títulos menos buscados/populares.

Asumiendo que el trayecto de la ruta AS de peering y hacia el OCA son iguales, y si usted anuncia los mismos prefijos en la sesión de peering pública o privada (usando AS2906) y en el OCA (usando AS40027), se preferirá el OCA en lugar de peering. Esto es porque el plano de control tendrá dos registros BGP para ese prefijo:

- Uno con trayecto AS PATH de 1 (<AS\_NUMBER>) desde el dispositivo
- Uno con trayecto AS PATH de 2 (2906 <AS\_NUMBER>) desde el sitio de peering

Tenga en cuenta el criterio de selección descrito anteriormente, y recuerde que en general se recomienda anunciar las rutas más específicas a sus dispositivos, para que así éstos tengan preferencia al momento de servir tráfico.

## ARQUITECTURA DE CLUSTER

Cuando hay más de un OCA en un sitio, estos dispositivos son configurados como un clúster de manifiesto único. Los OCAs en un clúster de manifiesto comparten el contenido almacenado y funcionan juntos como una sola unidad lógica.

A pesar de que los socios no necesitan configurar los clústeres de manifiesto, es importante entender algunos conceptos básicos de clustering. Sobre todo porque hay implicaciones que considerar cuando los dispositivos en un clúster son movidos a otro sitio o cuando se les da mantenimiento.

Los beneficios de clustering:

- **Mayor descarga para contenido único**

En un clúster típico de dos OCAs, ambos dispositivos utilizarán aproximadamente 40% de su capacidad para almacenar el mismo contenido popular. Este contenido representa apenas el 60% del total de descarga del dispositivo. El 60% restante del espacio de almacenamiento de cada OCA se usa para almacenar el contenido que se accede con menor frecuencia. El mismo set de contenido no se almacena en cada OCA de un clúster, debido a eso un clúster de OCAs ofrece mayor descarga total que un conjunto de OCAs que no han sido agrupados en un clúster. Esta estrategia permite que los OCAs en un mismo sitio operen de manera más eficiente.

Puede encontrar más información sobre estrategias de almacenamiento en este [artículo](#) de Netflix TechBlog.

- **Mayor resiliencia**

En un clúster con dos OCAs hay redundancia. En caso de que un OCA falle, el dispositivo saludable se hará cargo de la mayoría del tráfico que la unidad fallida estaba sirviendo. Vea los diferentes escenarios de fallos en [ejemplos de arquitecturas](#).

## AVISO IMPORTANTE A LOS SOCIOS

- Una vez que un conjunto de OCAs ha sido instalado en un sitio y agrupado como un clúster por el equipo de Open Connect, éste conjunto de OCAs debe ser visto como un solo servidor. Por lo tanto, cualquier cambio que se haga en un OCA dentro de un sitio puede impactar de forma negativa la eficiencia de servicio y comportamiento de todo el grupo.
- Si necesita hacer cambios en los OCAs en un sitio - por ejemplo, si necesita trasladar un OCA de un sitio a otro, o si requiere desactivar uno o más OCAs por un período de tiempo largo - es importante que notifique al equipo de Open Connect para que se hagan los cambios necesarios a la configuración del clúster. No hacerlo, puede ocasionar consecuencias no deseadas. Por ejemplo, el tráfico puede ser direccionado hacia el sitio equivocado, los patrones de tráfico pueden llegar a ser subóptimos, y se pueden desarrollar puntos de cuello de botella.
- Para facilitar patrones de tráfico óptimos y equilibrados, los OCAs en un sitio deben recibir exactamente los mismos anuncios BGP. Por lo tanto, si un OCA se reubica a otro sitio, debe revisar las rutas anunciadas en el dispositivo para asegurar que el tráfico sea direccionado de forma adecuada.

## DISPOSITIVOS FLASH

Si usted es un ISP con niveles altos de tráfico de Netflix, podemos incluir dispositivos Flash en la arquitectura de despliegue de OCAs. Los dispositivos Flash se ofrecen cuando se alcanza el límite de dispositivos Storage.

Article is closed for comments.



OPEN CONNECT

## Configuração de rede

English version: [Network configuration](#)

Esta seção descreve como os dispositivos Open Connect (OCA, Open Connect Appliance) são normalmente configurados em uma rede. Se você é um parceiro de ISP Open Connect, a Netflix trabalha em próxima colaboração com você para determinar a configuração ideal para suas necessidades específicas.

Para mais informações, consulte as [perguntas frequentes \(FAQs\)](#)

- [Visão geral](#)
- [Configuração da interface do roteador](#)
- [Reconfiguring the IP address of an OCA](#)
- [Roteamento e direção de conteúdo por meio de anúncios BGP](#)
- [Arquiteturas de agrupamento](#)
- [Aparelhos baseados em Flash](#)

## VISÃO GERAL

As OCAs são *aparelhos de cache direcionados* (directed cache appliances), o que significa que a maneira pela qual o tráfego é direcionado para o aparelho é determinada explicitamente por você e pela Netflix, não pelo próprio aparelho.

Uma OCA atende apenas clientes em endereços IP que você anuncia para a OCA por meio de uma sessão BGP. Em outras palavras, o tráfego só é entregue das suas OCAs incorporadas para os prefixos de clientes que você anuncia explicitamente a elas, conforme descrito nas seções a seguir. Portanto, você, como ISP parceiro, tem controle total sobre as redes que os aparelhos servirão. As sessões BGP são estabelecidas entre o(s) aparelho(s) e o roteador conectado mais próximo.

Se for solicitado conteúdo que não esteja contido em uma OCA incorporada, a solicitação do cliente será direcionada para o site de conteúdo da Netflix mais próximo via peering (se presente) ou via trânsito.

## RECONFIGURANDO O ENDEREÇO IP DE UM OCA

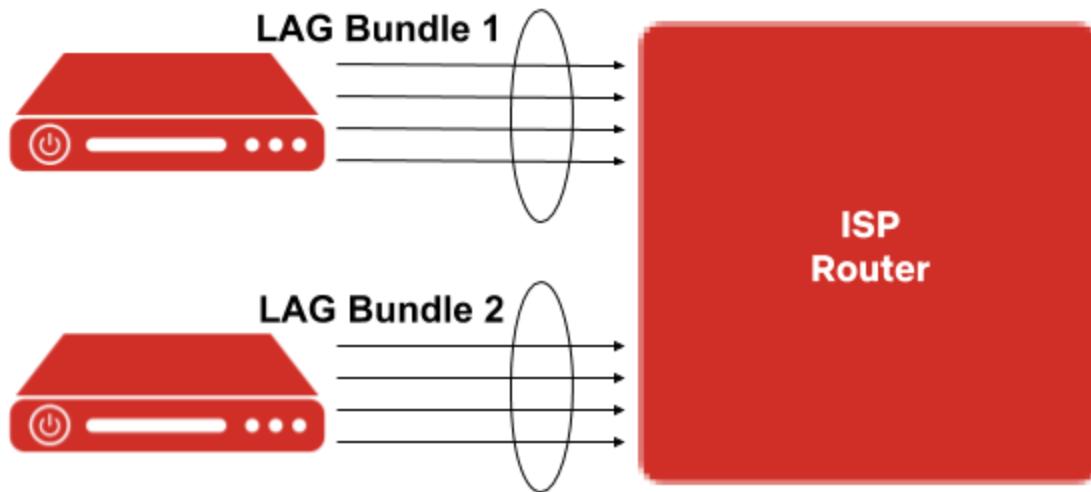
Cada dispositivo vem totalmente configurado com base nos detalhes do endereço IP que você forneceu à Netflix na enquete do seu site antes de ser enviado.

Para obter instruções passo a passo sobre como alterar o endereço IP de uma OCA, consulte o seguinte artigo: [Atualizando o endereço IP de um OCA](#)

## CONFIGURAÇÃO DA INTERFACE DO ROTEADOR

Quando você estiver conectando os aparelhos ao seu roteador, siga as diretrizes desta seção. Veja também [Exemplos de configurações de roteador](#).

- Cada OCA deve receber um endereço IPV4 roteável publicamente, e é altamente recomendável configurar também um endereço IPV6.
- Você pode configurar um endereço ao dispositivo a partir de uma sub-rede IPv4 de /31 e maior, ou uma sub-rede IPv6 de /127 e maior.
- É aceitável configurar um endereço ao aparelho a partir de uma sub-rede maior (por exemplo, um /24). Como apenas um endereço IPv4 é necessário por dispositivo, normalmente é usada uma sub-rede menor.
- As interfaces do roteador devem ser configuradas para o Link Aggregation Group (LAG) com LACP. Cada servidor deve ser configurado em seu próprio grupamento LAG para as interfaces ativas em cada servidor, conforme ilustrado no diagrama abaixo. Na configuração de exemplo de dois servidores, existem dois grupamentos LAG separados, um para cada servidor.



- Uma unidade de transmissão máxima padrão (maximum transmission unit, MTU) deve ser configurada em cada interface do roteador. Quadros Jumbo (jumbo frames) não são suportados.
- Se houver vários roteadores disponíveis que possam fornecer redundância em um site, recomenda-se escalar os aparelhos entre os roteadores. Os aparelhos no mesmo roteador devem estar na mesma sub-rede para otimizar o preenchimento. Os aparelhos em roteadores separados devem estar em sub-redes separadas. Os aparelhos não são projetados para serem conectados a dois roteadores separados.
- Todas as portas em uma OCA devem estar conectadas ao mesmo roteador ou switch. O uso de LAG multi-chassi ou empilhamento de switches não é suportado.
- Cada OCA é configurado para ser protegido contra ataques de rede e é projetado para ser conectado diretamente à internet. A filtragem do tráfego de entrada ou saída pode causar problemas operacionais, por isso recomendamos que você permita todo o tráfego em todas as portas, não use ACLs e garanta que seu roteador tenha uma rota padrão (default route) ou uma tabela de roteamento completa. Se você absolutamente **precisar** filtrar, a lista atual de uso de entrada e saída segue. Observe que estas portas podem mudar a qualquer momento sem notificação prévia.
  - **Tráfego da OCA:** Permitir todos os endereços e portas de destino.
  - **Tráfego para OCA:** Permita TCP 22, 53, 80, 179, 443, UDP 53 e 123 (fonte e destino), tipos ICMP 0, 3, 8, 11 e todos os ICMPv6 de qualquer IP/porta pública. Permitir todo o tráfego de retorno de qualquer conexão iniciada pelo aparelho (TCP estabelecido).

- **Nota:** Você pode confirmar o status da conectividade OCA de entrada/saída necessária [no Portal do Parceiro](#) (Partner Portal).
- Cada interface de rede deve receber entre 0 dBm e -10 dBm de luz para garantir uma boa taxa de transferência de dados. O painel LCD na frente do aparelho exibe os níveis de luz atuais para cada interface. Se o seu dispositivo não tiver um painel LCD, acesse o console com um teclado e mouse.
  - Para mais informações, consulte os seguintes artigos relacionados:
    - [Verificando a intensidade do sinal óptico em uma OCA](#)
    - [Solução de problemas de erros de entrada ou baixos níveis de luz em uma OCA](#)

## ROTEAMENTO E DIREÇÃO DE CONTEÚDO VIA ANÚNCIOS BGP

Direcionamos os clientes para nossas OCAs com base nos anúncios BGP de um ISP, juntamente com os algoritmos de roteamento e direção no plano de controle Open Connect. Os ISPs parceiros podem controlar alguns aspectos da direção de conteúdo por meio das rotas BGP que são anunciadas via peering ou para cada OCA incorporada.

O plano de controle encaminha os clientes para as melhores OCAs disponíveis usando uma versão modificada da melhor seleção de caminho do BGP. Supondo que o dispositivo tenha o título solicitado e a capacidade de serviço disponível, o plano de controle fornece aos clientes uma lista classificada de dispositivos (normalmente 3 ou mais fontes confiáveis) dos quais fazer streaming.

## CRITÉRIOS DE SELEÇÃO DE APARELHOS

Os seguintes critérios de seleção de aparelhos são considerados, em ordem, pelos serviços do plano de controle Open Connect. Se houver um empate para um determinado critério, então o próximo critério é considerado. Se houver um empate em todos os critérios, o tráfego será equilibrado entre os aparelhos.

1. O dispositivo que recebe a rota mais específica para o prefixo do cliente.
2. O dispositivo que recebe a rota para o netblock do cliente com o caminho AS mais curto. (Veja as [notas sobre peering](#) abaixo).
3. O dispositivo que recebe a rota para o netblock do cliente com o menor discriminador de múltiplas saídas (multi-exit discriminator, MED). (Veja as [notas sobre MEDs](#) abaixo).
4. O aparelho geograficamente mais próximo\*. A geolocalização é feita em base nos IPs do cliente, e essa localização é comparada com à latitude e longitude das OCAs próximas para determinar o sistema disponível mais próximo.

**\*Nota:** Se você tiver duas sites redundantes com OCAS instaladas na sua própria rede que estão geograficamente bem conectados **e** forem projetados para atender ao mesmo conjunto de clientes (com os mesmos prefixos anunciados para as duas sites), é possível que a Netflix defina uma substituição geográfica para que o tráfego seja igualmente equilibrado em as dois sites. Se você tiver essa situação, pode [abrir um ticket](#) para solicitar uma substituição geográfica.

## NOTAS ADICIONAIS SOBRE MEDS

- Honramos os valores MED que recebemos. Leve nota que aumentamos o valor da seguinte forma, dependendo de onde aprendemos o prefixo:
  - +0 para um OCA instalado dentro da sua rede (servidor Netflix Cache)
  - +50 para uma conexão de peering direta (PNI)
  - +100 para peering em um IX (peering público)
- Não há limite para o valor máximo de MED.

- Um MED ausente é tratado da mesma forma que um MED de 0 e indica que o aparelho deve receber todo o tráfego a ser servido para os prefixos associados (também muitas vezes referido como *MED-missing-as-best*). Lembre-se, se vários dispositivos receberem o mesmo prefixo com a mesma métrica, o tráfego será equilibrado em carga entre esses aparelhos. Como um MED ausente será equivalente a 0, é preferível a qualquer MED >0 em outros aparelhos.
- **Importante:** Marcar MEDs em dispositivos Open Connect já instalados e funcionando pode ser perigoso, porque deve ser feito em todas as sessões BGP para todos os dispositivos ao mesmo tempo.

Finalmente, um lembrete de que, se você tiver uma conexão de peering com a Netflix e fizer filtragem IRR, nosso prefix-set é RS-NETFLIX e nosso AS-SET é AS-NFLX. Certifique-se de aceitar anúncios que se originam de ASNs: 2906, 40027 e 55095.

Veja também: [Locais de Peering](#).

## REQUISITOS BGP

- Anúncios de rota para OCAs instaladas na sua própria rede:
  - Prefixos IPv4 entre /8 e /31 (inclusivo) são aceitos.
  - Prefixos IPv6 entre /19 e /64 (inclusivo) são aceitos.
- Anúncios de rota para sessões de peering Open Connect:
  - Prefixos IPv4 entre /8 e /24 (inclusivo) são aceitos.
  - Prefixos IPv6 entre /19 e /48 (inclusivo) são aceitos.
- Como requisito implícito, **todos os** aparelhos devem ter uma sessão BGP configurada para participar corretamente da direção e entrega de conteúdo da Netflix.
- Para localizar o tráfego, a melhor prática é anunciar as rotas mais específicas para o aparelho. Por exemplo, se você estiver anunciando um /22 para a OCA, mas um /24 for recebido do mesmo bloco sobre peering ou trânsito de conexão direta gratuita (SFI - settlement-free interconnection), o /24 será preferido, entregando tráfego de conteúdo da fonte remota em vez da OCA.
- Se estiver instalando apenas uma OCA em sua rede, você deverá anunciar o prefixo mais específico (mais longo) para essa OCA na sessão de peering que deseja que a OCA use para fins de preenchimento noturno.
- Se você estiver implantando várias OCAs em mais de um site em sua rede:
  - Para permitir o preenchimento noturno eficiente: certifique-se de que os aparelhos dentro de um site possam ouvir as sub-redes dos aparelhos no outro site por meio da conexão BGP estabelecida com o seu roteador. Consulte as informações de [preenchimento e atualizações](#) para obter mais detalhes.
  - Veja as informações adicionais sobre [arquiteturas de agrupamento](#).
- A Netflix não usa nenhuma informação da comunidade BGP que seja anunciada por parceiros para OCAs ou via peering Open Connect.
- Rotas anunciadas que são recebidas por uma OCA são sincronizadas com os serviços de plano de controle Open Connect aproximadamente a cada cinco minutos.
- Se você pretende servir o tráfego do cliente das OCAs instaladas na sua própria rede para prefixos dentro de um ASN que está fora da sua rede, certifique-se de que você está [Documentando Relacionamentos de Rede com um AS-SET](#)
- A Netflix usa filtragem de rotas baseada em RPKI. Para mais informações, consulte: [Filtragem de rota baseada em RPKI](#).

- A Netflix se juntou à iniciativa MANRS. Para mais informações, consulte: [Mutually Agreed Norms for Routing Security \(MANRS\)](#)

## SOLUÇÃO DE PROBLEMAS DE ANÚNCIOS BGP

Existem algumas ferramentas no Portal de Parceiros que você pode usar para explorar e solucionar problemas de anúncios do BGP:

- Use o [Route Explorer](#) para monitorar o estado das sessões e anúncios do BGP que você configurou entre seus roteadores e os dispositivos Netflix Open Connect instalados na sua própria rede.
- Use o [Route Optimizer](#) para executar relatórios em seus anúncios de rota BGP. Os relatórios [do Route Optimizer](#) incluem todos os anúncios que a Netflix ouve de seus ASN(s), incluindo em sites peering e OCAs instalados na sua própria rede.
- Veja o [Route Performance Report](#) para descobrir prefixos em sua rede que estão potencialmente experimentando uma qualidade de streaming de vídeo relativamente baixa.

## OCAS INSTALADAS NA SUA PRÓPRIA REDE COM CONEXOES DE PEERING

A implementação ideal do Open Connect é uma mistura de peering SFI e OCAs incorporadas. A Netflix usa dois sistemas autônomos separados para peering:

- AS2906 é o número AS que a Netflix usa para peering em seus PoPs
- AS40027 é o número AS que as OCAs dentro da sua própria rede usam para peering com redes ISP

Consulte [os requisitos do BGP](#) para anúncios de prefixo que são aceitos em sessões de peering.

Quando o peering OCAs e Open Connect SFI são combinados, o peering é usado principalmente para backup, preenchimento e serviço de títulos de cauda longa (*long-tail titles*).

Supondo que o AS PATH LENGTH para uma OCA instalada na sua própria rede e o peering sejam iguais, se você anunciar o mesmo prefixo tanto para uma sessão de peering privada ou pública (usando AS2906) quanto para um OCA (usando AS40027), a OCA será preferida ao peering. Isso ocorre porque o plano de controle Open Connect terá duas entradas BGP para esse prefixo:

- um com o próprio aparelho
- um com o local do peering

Tenha em mente os [critérios de seleção de aparelhos](#) acima e lembre-se de que a melhor prática geral é anunciar rotas mais específicas para OCAs instaladas na sua própria rede para que eles sejam preferidos para atender o tráfego.

## ARQUITETURAS DE CLUSTERING

O número de OCAs instaladas em cada site dentro da sua rede dependerá do volume de tráfego da Netflix sendo servido a partir do site. Em muitos casos, um único OCA é suficiente. Entanto, se o volume de tráfego justificar OCAs adicionais dentro de um site, nós as configuramos como um único cluster de catálogo. As OCAs em um cluster de catálogo compartilham armazenamento de conteúdo e funcionam juntas como um servidor/unidade de armazenamento lógico.

Embora os parceiros não precisem configurar *clusters de manifesto*, é importante entender alguns conceitos básicos de agrupamento. Em particular, há implicações a serem consideradas quando as OCAs em um cluster são retirados para manutenção ou movidos para um local diferente.

O agrupamento dos OCAs dentro de um site permite uma maior descarga de conteúdo exclusivo. Em um cluster de duas OCA, ambos os aparelhos usarão aproximadamente 40% de sua armazenamento para o mesmo conteúdo popular. Esse conteúdo popular normalmente representa cerca de 60% da descarga total da OCA. Os 60% restantes do espaço de armazenamento em cada OCA são usados para armazenar um conjunto exclusivo de conteúdo acessado com menos frequência. Como não armazenamos o mesmo conjunto exato de conteúdo em cada OCA em um cluster, um cluster de OCAs fornece maior descarga total do que um grupo de OCAs sem cluster. Essa estratégia ajuda as OCAs em um site a funcionar com mais eficiência.

Para mais informações sobre estratégias de armazenamento, consulte [este tech blog post](#).

## NOTAS IMPORTANTES PARA PARCEIROS:

- Depois que um conjunto de OCAs foi instalado em um site e agrupado como um cluster pela equipe Open Connect, eles devem ser considerados como um grande servidor. Portanto, quaisquer alterações que você fizer em um único OCA em um site têm o potencial de impactar negativamente a eficiência de serviço e o comportamento do grupo.
- Se você precisar fazer alterações nas OCAs em um site estabelecido - por exemplo, se você pretende realocar uma OCA de um site para outro ou desativar uma ou mais OCAs por um período significativo de tempo - é importante notificar a equipe do Open Connect para que eles possam fazer as alterações necessárias na configuração do cluster. Não fazer isso pode causar consequências indesejadas. Por exemplo, você pode ver o tráfego sendo direcionado para o site errado, os padrões de preenchimento podem se tornar subótimos e os pontos quentes podem se desenvolver.
- Para permitir padrões de tráfego ideais e equilibrados, as OCAs em um site devem receber exatamente os mesmos anúncios de rota BGP. Portanto, se você realocar uma OCA, deverá revisitar seus anúncios de rota BGP para garantir que o tráfego continue a ser direcionado adequadamente.

## APARELHOS BASEADOS EM FLASH

Se você é um ISP com grandes quantidades de tráfego da Netflix, podemos incluir dispositivos baseados em flash em sua arquitetura de implantação OCA. Os dispositivos baseados em Flash são servidores baseados em memória flash que são instalados quando você atinge um número limite de OCAs, para aumentar a capacidade de entrega dos dispositivos principais (de armazenamento).

Article is closed for comments.



OPEN CONNECT

## Example router configurations

Use the following examples to help you understand typical router configurations.

- [Arista EOS example](#)
- [Brocade LAG BGP example](#)
- [Cisco IOS BGP example](#)
- [Cisco IOS XR BGP example](#)
- [Cisco IOS XR LACP example](#)
- [Cisco IOS Interface LACP example](#)
- [Cisco IOS XR Bridged Interface example](#)
- [Cisco IOS Switch with VLAN example](#)
- [Junos BGP example](#)
- [Junos Interface LACP example](#)
- [Junos Bridged Interface example](#)

### ARISTA EOS EXAMPLE CONFIGURATION

```
!
router BGP <ASN>
neighbor <IP address of Appliance> remote-as 40027
neighbor <IP address of Appliance> route-map NETFLIX-OUT out
!
route-map NETFLIX-OUT permit 10
match ip address prefix-list NETFLIX-LOCAL
set metric 0
!
route-map NETFLIX-OUT permit 20
match ip address prefix-list NETFLIX-BACKUP
set metric 100
!
route-map NETFLIX-OUT deny 30
!
```

### BROCADE LAG BGP EXAMPLE CONFIGURATION

```
lag "NETFLIX" dynamic
ports ethernet 1/7 to 1/8
primary-port 1/7
deploy
port-name "NETFLIX-OCA" ethernet 1/7
port-name "NETFLIX-OCA" ethernet 1/8
interface ethernet 1/7
```

```

enable
ip address <interface address/mask>
no ip redirect
ipv6 address <interface address/mask>
sflow forwarding
link-aggregate active
interface ethernet 1/8
enable
link-aggregate active

router bgp
neighbor Netflix peer-group
neighbor Netflix remote-as 40027
neighbor NetflixIPv6 peer-group
neighbor NetflixIPv6 remote-as 40027
neighbor <IPv4 address of Appliance> peer-group Netflix
neighbor <IPv4 address of Appliance> description "Netflix Open Cache Appliance"
neighbor <IPv6 address of Appliance> peer-group NetflixIPv6
neighbor <IPv6 address of Appliance> description "Netflix Open Cache Appliance"

address-family ipv4 unicast
neighbor Netflix prefix-list no-advertise in
neighbor Netflix prefix-list NETFLIX-LOCAL out
no neighbor NetflixIPv6 activate
exit-address-family

address-family ipv6 unicast
neighbor NetflixIPv6 activate
neighbor NetflixIPv6 prefix-list no-advertise-ipv6 in
neighbor NetflixIPv6 prefix-list NETFLIX-LOCAL-IPV6 out
exit-address-family

```

## CISCO IOS BGP EXAMPLE CONFIGURATION

```

!
router BGP <ASN>
neighbor <IP address of Appliance> remote-as 40027
neighbor <IP address of Appliance> route-map NETFLIX-OUT out
!
route-map NETFLIX-OUT permit 10
match ip address prefix-list NETFLIX-LOCAL
set metric 0
!
route-map NETFLIX-OUT permit 20
match ip address prefix-list NETFLIX-BACKUP
set metric 100
!
route-map NETFLIX-OUT deny 30
!
```

## CISCO IOS XR BGP EXAMPLE CONFIGURATION

```

!
router bgp <ASN>
neighbor <IP address of Appliance>
remote-as 40027
address-family ipv4 unicast
route-policy NETFLIX-OUT out
!
```

```

route-policy NETFLIX-OUT
if destination in NETFLIX-LOCAL then
set med 0
elseif destination in NETFLIX-BACKUP then
set med 100
else
drop
endif
end-policy
!
prefix-set NETFLIX-LOCAL
192.0.2.0/25,
192.168.100.0/25
end-set
!
prefix-set NETFLIX-BACKUP
192.0.2.128/25,
192.168.100.128/25
end-set
!
```

## CISCO IOS XR LACP EXAMPLE CONFIGURATION

```

!
interface Bundle-Ether1
bundle minimum-active bandwidth 1
ipv4 address <address/mask>
ipv6 address <really-long-address/mask>
!
interface TenGigE0/0/2/0
bundle id 1 mode active
lacp period short
!
interface TenGigE0/0/2/2
bundle id 1 mode active
lacp period short
!
```

## CISCO IOS INTERFACE LACP EXAMPLE CONFIGURATION

```

!
interface Port-channel1
ip address <address> <mask>
!
interface GigabitEthernet1/1
channel-group 1 mode active
channel-protocol lACP
!
interface GigabitEthernet1/2
channel-group 1 mode active
channel-protocol lACP
!
```

## CISCO IOS XR BRIDGED INTERFACE EXAMPLE CONFIGURATION

For multiple servers with LAG, using the same default gateway.

```
interface BVI100
description NETFLIX
ipv4 address <address/mask>
ipv6 address <really-long-address/mask>
```

```
I2vpn
load-balancing flow src-dst-ip
bridge group NETFLIX-OCAS
bridge-domain NETFLIX-OCAS
interface Bundle-Ether1
interface Bundle-Ether2
routed interface BVI100
```

```
interface Bundle-Ether1
I2transport
interface Bundle-Ether2
I2transport
```

## CISCO IOS SWITCH WITH VLAN EXAMPLE CONFIGURATION

For multiple servers in LAG groups, behind a switch.

```
! SVI Configuration
!
interface Vlan30
description **NETFLIX OCA SERVERS**
ip address <address/mask>

! Port channel configuration
!
interface Port-channel31
description **LINK TO NETFLIX-OCA-1**
switchport
switchport mode access
switchport access vlan 30
!
interface Port-channel32
description **LINK TO NETFLIX-OCA-2**
switchport
switchport mode access
switchport access vlan 30

! Interfaces configuration
!
! OCA1
interface TenGigabitEthernet1/1/1
description **LINK TO NETFLIX-OCA1-TENO**
switchport
switchport mode access
switchport access vlan 30
channel-group 31 mode active
!
interface TenGigabitEthernet1/1/2
description **LINK TO NETFLIX-OCA1-TEN1**
switchport
switchport mode access
switchport access vlan 30
channel-group 31 mode active

! OCA2
```

```

interface TenGigabitEthernet2/1/1
description **LINK TO NETFLIX-OCA2-TENO**
switchport
switchport mode access
switchport access vlan 30
channel-group 32 mode active
!
interface TenGigabitEthernet2/1/2
description **LINK TO NETFLIX-OCA2-TEN1**
switchport
switchport mode access
switchport access vlan 30
channel-group 32 mode active

```

## JUNOS BGP EXAMPLE CONFIGURATION

```

protocols {
    bgp {
        group NETFLIX {
            neighbor <IP address of Appliance> {
                export NETFLIX-EXPORT;
                peer-as 40027;
            }
        }
    }
}

policy-options {
    policy-statement NETFLIX-EXPORT {
        term NETFLIX-LOCAL {
            from {
                prefix-list NETFLIX-LOCAL;
            }
            then {
                metric 0;
                accept;
            }
        }
        term NETFLIX-BACKUP {
            from {
                prefix-list NETFLIX-BACKUP;
            }
            then {
                metric 100;
                accept;
            }
        }
        then reject;
    }
}

```

## JUNOS INTERFACE LACP EXAMPLE CONFIGURATION

```

interfaces {
    ae1 {
        description NETFLIX-OCA;
        aggregated-ether-options {
            lACP {

```

```

        active;
        periodic fast;
    }
}
unit 0 {
    family inet {
        address <address/mask>;
    }
    family inet6 {
        address <really-long-address/mask>;
    }
}
}
xe-0/0/0 {
    description NETFLIX-OCA-cxgbe0;
    ether-options {
        802.3ad ae1;
    }
}
xe-0/0/1 {
    description NETFLIX-OCA-cxgbe1;
    ether-options {
        802.3ad ae1;
    }
}
}
}

```

## JUNOS BRIDGED INTERFACE EXAMPLE CONFIGURATION

For multiple servers with LAG, using the same default gateway

```

vlans {
    NETFLIX-OCAS {
        vlan-id 100;
        l3-interface irb.100;
    }
}
interfaces {
    irb {
        unit 100 {
            family inet {
                address <address/mask>;
            }
            family inet6 {
                address <really-long-address/mask>;
            }
        }
    }
    ae0 {
        description NETFLIX-OCA-1;
        unit 0 {
            family ethernet-switching {
                vlan {
                    members NETFLIX-OCAS;
                }
            }
        }
    }
    ae1 {
        description NETFLIX-OCA-2;
    }
}

```

```
unit 0 {
    family ethernet-switching {
        vlan {
            members NETFLIX-OCAS;
        }
    }
}
xe-0/0/0 {
    description NETFLIX-OCA-1-PORT1;
    ether-options {
        802.3ad ae0;
    }
}
xe-0/0/1 {
    description NETFLIX-OCA-1-PORT2;
    ether-options {
        802.3ad ae0;
    }
}
xe-0/0/2 {
    description NETFLIX-OCA-2-PORT1;
    ether-options {
        802.3ad ae1;
    }
}
xe-0/0/3 {
    description NETFLIX-OCA-2-PORT2;
    ether-options {
        802.3ad ae1;
    }
}
```

Article is closed for comments.



OPEN CONNECT

## Turn-up checks for OCA deployments

During the burn-in period of OCA deployment, multiple checks are run on the appliance. You will receive periodic emails with the results of the checks, which run approximately every 24 hours until all checks pass.

The current state of the deployment and turn-up checks is displayed in the Partner Portal on the **Overview** page for each OCA that is under deployment.

The screenshot shows the Netflix Partner Portal interface. At the top, there's a header with the Netflix logo and 'OPEN CONNECT'. Below the header, a section titled 'Turn-up checks for OCA deployments' displays a table with one row. The table has columns for 'Problem' (containing a red exclamation mark icon and 'Network Errors'), 'Description' (containing 'Network InErrors detected on TEN0. Try cleaning or replacing the fi...', 'Failed at 2022-09-02 12:08:22, Next check at 2022-09-02 14:08:22'), and 'Help' (containing a three-dot menu icon). Below the table, there are navigation links: 'Tickets' (with a '1' notification), 'Audit Log', and 'Forms'. The main content area is titled 'Deployment New Appliance' and shows a vertical checklist: 'Preparing for Shipment' (checked), 'Shipped' (checked), 'Delivered' (checked), and 'In Turn-up' (checked, highlighted with a blue border and labeled 'Action Required'). A note below the checklist states: 'The OCA is in the process of being turned up to serve traffic. This process typically takes approximately 2 days after all checks pass.' A footer at the bottom of this section shows '20/21 checks passing'.

The appliance will not start serving client traffic until all checks pass and acceptable offload can be achieved. When the system is ready, the Netflix Open Connect Operations team will automatically enable the system to serve clients and will continue to monitor its performance. At this point, we will start monitoring and flagging a **similar set of Live checks**.

This article provides detailed information about each turn-up check:

- Network Interface and PSU Checks
- Connectivity and Reachability Checks

- [Fill Checks](#)
- [BGP and Traffic Checks](#)
- [Incomplete OCA Return Form](#)

# Network Interface and PSU Checks

Several checks verify that the network interfaces and power supply units (PSUs) that were included with the OCA were properly installed, are functional, and are not flapping or reporting errors. For general instructions and troubleshooting information for network interface errors, see the following related articles:

- For instructions on how to physically install optics connectors, see [Removing or replacing an optics connector](#)
- For additional troubleshooting information, see [Troubleshooting input errors or low light levels on an OCA](#)

## NETWORK CONFIGURATION

This check verifies that the expected number of network interfaces are present and that light levels are adequate.

### TROUBLESHOOTING NOTES:

- OCAs are shipped to you with the expected number of supported optics connectors and cables. You should only use the parts that were included in the shipment, and ensure that you install and cable all included optics.
- Only single-mode or multi-mode fiber connections are supported. Direct Attach cabling (also known as DAC, TwinAx, CR, Cu, or copper) is incompatible.
- If you have replaced the optical modules due to incorrect part types being requested or delivered, please [open a ticket](#) to request that new optics be shipped to you.
- Follow the general instructions and troubleshooting information [above](#) as needed.

## NETWORK ERRORS

This check verifies that there are no input errors on the network interfaces.

### TROUBLESHOOTING NOTES:

- You can [view input errors in the Partner Portal](#), on the **Metrics** page for each OCA.
- Follow the general instructions and troubleshooting information [above](#) as needed.

## NETWORK FLAPS

This check verifies that the network interfaces are not flapping.

### TROUBLESHOOTING NOTES:

- You can [check for interface flaps in the Partner Portal](#), on the **Metrics** page for each OCA.
- Follow the general instructions and troubleshooting information [above](#) as needed.

## POWER SUPPLIES

This check verifies that the installed power supply(s) (PSUs) that were included with the OCA are functioning and reporting their status appropriately to our monitoring systems.

### TROUBLESHOOTING NOTES:

- For instructions on how to physically install PSUs, see [Removing or replacing a power supply unit](#)
- For additional troubleshooting information, see [Troubleshooting Power Supply Unit \(PSU\) issues](#)
- Some OCA Versions do not reliably report PSU status, in which case this check is skipped.

---

# Connectivity and Reachability Checks

The following series of checks verify that the OCA has the required connectivity to serve Netflix traffic, communicate with our control plane services in AWS, and can be successfully reached for monitoring and administrative tasks. When you are troubleshooting connectivity issues:

- Ensure that all required ports are open as described in the [Network configuration](#) section of the Deployment Guide.
- Ensure there are no firewalls, proxies, anti-DDoS protection, or third party caching infrastructure installed that may be interfering with connectivity.
- For additional troubleshooting information, see [Viewing connectivity metrics for an OCA](#)

## HTTP CONNECTIVITY

This check verifies basic HTTP connectivity by making a request and verifying that the expected response code is returned. This connectivity is required to communicate with our control plane services and to serve Netflix traffic.

### TROUBLESHOOTING NOTES:

- Follow the general connectivity troubleshooting information [above](#).

## BASIC REACHABILITY

This check verifies that the OCA responds to pings from outside your network.

### TROUBLESHOOTING NOTES:

- Ensure that the OCA has been assigned a publicly-routable IPv4 address as described in the [Router Interface Configuration section of the Network Configuration article](#).
- Ensure that ICMP traffic is not being blocked.
- Follow the general connectivity troubleshooting information [above](#).

## SSH MANAGEABILITY

This check verifies that the OCA is reachable via SSH from our AWS instances. This connectivity is required for monitoring and administrative tasks.

### TROUBLESHOOTING NOTES:

- Follow the general connectivity troubleshooting information [above](#).

## IPMI CONFIGURATION

This check verifies that the OCA is able to communicate with the Netflix endpoint that performs IPMI bundle updates.

### TROUBLESHOOTING NOTES:

- Verify that there are no firewalls, filters or ACLs which are preventing access to <https://hw-oca.oc.netflix.com>.
- Follow the general connectivity troubleshooting information [above](#).

## NTP SYNCHRONIZATION

This check verifies that the OCA is able to properly synchronize its clock using Network Time Protocol (NTP).

### TROUBLESHOOTING NOTES:

- Ensure that UDP port 123 (and all other required ports as described [above](#)) is open.
- Follow the general connectivity troubleshooting information [above](#).

---

# Fill Checks

The following checks verify that the OCA is able to download content updates (nightly fill) at the required speed. For general information and requirements for fill traffic, see the following articles:

- [Fill patterns](#)
- [Is it possible to expand the fill window or set OCAs to fill faster?](#)
- [How do the appliances determine where to receive update or fill content from?](#)

## FILL PERFORMANCE

This check verifies that the OCA is successfully able to request and download a sufficient percentage of required content updates during the fill window.

### TROUBLESHOOTING NOTES:

- Ensure that there are no [errors on your network interfaces](#), or heavy congestion between the site and Netflix fill sites on the internet during the fill window.

- Consult the general fill information [above](#) as needed.

## FILL SPEED

This check verifies that the OCA is able to download content updates at the required speed.

### TROUBLESHOOTING NOTES:

- Ensure that there are no [errors on your network interfaces](#), or heavy congestion between the site and Netflix fill sites on the internet during the fill window.
- Consult the general fill information [above](#) as needed.

---

## BGP and Traffic Checks

The following checks validate that the OCA has an established BGP session and is learning and reporting routes. BGP must be configured properly so that the OCA can serve Netflix traffic to client devices within your network. For general information about BGP configurations and advertisements, see the following information:

- [Network configuration - Routing and Steering via BGP Announcements](#)

## BGP IPV4/IPV6, UNEXPECTED BGP CONNECTION ATTEMPTS

These checks validate that IPv4 / IPv6 BGP sessions between the OCA and its BGP peer are properly configured and established, and verifies that the OCA is learning advertised routes via its BGP session(s). A failing check for **Unexpected BGP Connection Attempts** indicates that the OCA is receiving BGP connection requests from outside of your ASN.

### TROUBLESHOOTING NOTES:

- OCAs are configured before they are shipped, based on the network and BGP configurations that [you specified in the Site Survey form](#). Ensure that the configuration is expected and correct after installation.
- After the OCA begins reporting data to our control plane, you can view network and BGP configurations [in the Open Connect Partner Portal](#).
- You can view the routes that are being heard by each OCA and look for route inconsistencies within a site using the [Route Explorer](#) tool.
- If you need to make changes to the network configuration or BGP session configuration for an OCA after delivery and installation, follow [these steps](#).

## INCONSISTENT BGP ADVERTISEMENTS

This check verifies that all OCAs within the site are learning the same number of routes. All OCAs in the same site must serve the same customers and receive identical BGP prefix advertisements.

### TROUBLESHOOTING NOTES:

- You can view the routes that are being heard by each OCA and look for route inconsistencies within a site using the [Route Explorer](#) tool.

## TRAFFIC LEVELS

During the end of the burn-in cycle, the OCA will start to serve live test traffic when it is able to do so. This check verifies that test traffic is being served at the levels that were predicted during the site design process with the Open Connect team.

### TROUBLESHOOTING NOTES:

- Ensure that you are advertising via BGP to the OCA all of the routes that you plan to serve from the site.
- You can view the routes that are being heard by each OCA and look for route inconsistencies within a site using the [Route Explorer](#) tool.
- If traffic patterns have changed since you discussed them with us and you feel that the traffic levels reported in this check are expected, [open a ticket](#) to get help with this issue.

---

## Incomplete OCA Return Form (if applicable)

If this OCA is a replacement for a failed OCA via our [RMA return process](#) and we are requesting that you return the failed OCA, this check will run. In most cases, we ask you to E-Waste the failed OCA, but in some cases we ask that you return the failed OCA to Netflix for analysis and repair. This check verifies that the required OCA Return Form has been completed in our [Partner Forms](#) application.

### NOTES:

- You can view and link to all incomplete forms from [within the Partner Portal](#).
- For tips on filling out forms, see: [Getting started with Partner Forms](#)
- If you need help with the OCA return process, [open a ticket](#).

Article is closed for comments.



OPEN CONNECT

## Documenting Network Relationships with an AS-SET

If you want to advertise prefixes from another network (ASN) to your embedded OCA(s), you should first ensure that you have created an AS-SET in your internet routing registry (IRR) record that includes the ASN(s) that are associated with those prefixes.

**Note:** When you set up your AS-SET record, refer to the "aut-num" object (routing record) that describes the routing policies for your ASN. The AS-SET record must have the same "mnt-by" handler (also known in some internet registries as the "admin-c") as the "aut-num" so that our systems can recognize and associate them.

**Important:** We will flag and filter any prefixes advertised to your OCAs from an ASN that you do not own or have not properly documented in an AS-SET hierarchy.

### WHAT IS THE BENEFIT OF USING AN AS-SET?

AS-SETS provide a mechanism for publicly documenting a customer relationship between autonomous systems (ASNs). By creating an AS-SET with a members attribute that includes each network (ASN) with which you have an established relationship (transit, peering, and so on), you can formally document the networks that are authorized and expected to be served from your OCA(s). As a result, Netflix will receive an unambiguous signal that all prefixes associated with the ASNs in your AS-SET are not leaked routes, but fully authorized and expected.

This will prevent us from erroneously filtering potentially leaked routes.

For more information on the importance and benefits of using AS-SETS, see this article:

<https://www.manrs.org/2022/12/why-network-operators-should-use-hierarchical-as-sets/>

### HOW CAN I VERIFY THAT MY AS-SET IS SET UP CORRECTLY?

To verify that your AS-SET is correctly defined, you can run a query via **RADb**.

### HOW CAN I TELL WHICH OF MY ADVERTISED PREFIXES ARE BEING FLAGGED OR FILTERED?

Use the **Discover Unregistered Routes** report and the **View Filtered Routes** report in the **Partner Portal Route Optimizer** to identify the prefixes that we are flagging, and prefixes that we are filtering.

### WHAT IF I HAVE A DOWNSTREAM CUSTOMER, AND THEY ALSO HAVE DOWNSTREAM CUSTOMERS?

In this case, you should add a reference to your downstream customer's AS-SET in your AS-SET. Their AS-SET should in turn list all of the downstream ASNs that they have a relationship with.

### ISN'T MY PEERINGDB RECORD SUFFICIENT TO DOCUMENT MY NETWORK RELATIONSHIPS? DO I REALLY NEED TO CREATE AN AS-SET?

PeeringDB stores information about peering relationships, and we do use peeringDB as a source to determine ASN ownership of prefixes. However, it is not sufficient as a single data source. We use registered AS-SET hierarchies to verify relationships between ASNs.

## MORE INFORMATION

For more information about AS-SETs, see these additional resources:

[https://learn.nsrc.org/bgp/irr\\_objects](https://learn.nsrc.org/bgp/irr_objects)

<https://www.apnic.net/manage-ip/using-whois/guide/as-set/>

Article is closed for comments.



OPEN CONNECT

## AS-SET para documentar la relación entre redes

Si desea anunciar prefijos de otras redes (ASN) a los dispositivos OCA integrados en su red, debe asegurarse de tener un AS-SET creado en su registro de enrutamiento de internet (IRR) que incluya los ASNs asociados con esos prefijos.

**Nota:** Además del AS-SET, es necesario crear el objeto 'aut-num' (registro de enrutamiento), que describirá las políticas de enrutamiento para su ASN. Para que nuestro sistema pueda reconocer y asociar correctamente su AS-SET y aut-num, ambos registros deben incluir el mismo campo 'mnt-by' (también conocido como 'admin-c').

**Importante:** Los prefijos que se anuncien a sus OCAs y que pertenezcan a un ASN que no sea de su propiedad o cuya relación no esté documentada en su AS-SET serán filtrados.

### ¿CUÁL ES EL BENEFICIO DE USAR UN AS-SET?

Los AS-SET son un mecanismo que permite documentar de manera pública la relación entre diferentes sistemas autónomos (AS). Al establecer un AS-SET que incluya los ASN con los que mantiene relaciones (como tránsito o intercambio de tráfico), podrá documentar formalmente cuáles redes están autorizadas y se espera que sean atendidas por su OCA(s). Como resultado, Netflix recibirá una clara confirmación de que todos los prefijos asociados con los ASN en su AS-SET están completamente autorizados y no son sujetos a filtrado.

Esto evitirá el filtrado erróneo de rutas que deberían estar autorizadas.

Para obtener más información sobre la importancia y beneficios de un AS-SET, consulte el artículo:

<https://www.manrs.org/2022/12/why-network-operators-should-use-hierarchical-as-sets/>

### ¿CÓMO PUEDO VERIFICAR QUE MI AS-SET ESTÁ CONFIGURADO CORRECTAMENTE?

Para verificar que su AS-SET está definido de forma correcta, puede ejecutar una búsqueda a través de **RADb**.

### ¿CÓMO PUEDO SABER CUÁLES DE MI PREFIJOS ESTÁN MARCADO O SIENDO FILTRADOS?

Para identificar los prefijos que están siendo filtrados, en el Portal de Socios puede utilizar el reporte ver los reportes Descubrir Rutas no Registradas (Discover Unregistered Routes) y Ver Rutas Filtradas (View Filtered Routes) en la herramienta Optimizador de Rutas ([Partner Portal Route Optimizer](#))

### ¿QUÉ PASA SI TENGO UN CLIENTE DOWNSTREAM, Y ÉSTE TAMBIÉN TIENE CLIENTES DOWNSTREAM?

En ese caso, su AS-SET debe incluir una referencia del AS-SET de su cliente downstream. A su vez, el AS-SET de sus clientes debe incluir todos los ASNs downstream con los que tienen una relación.

## ¿ES SUFICIENTE TENER UN REGISTRO EN PEERINGDB PARA DOCUMENTAR MI RELACIÓN CON OTRAS REDES, O ES REALMENTE NECESARIO CONTAR CON UN AS-SET?

PeeringDB almacena información sobre las relaciones de intercambio de tráfico. Utilizamos PeeringDB para determinar la propiedad de los prefijos de un ASN. Sin embargo, PeeringDB no es suficiente para ser usado como una fuente única de datos. Utilizamos jerarquías de AS-SETS registrados para verificar las relaciones entre ASNs.

### INFORMACIÓN ADICIONAL

Para más información sobre AS-SETS, visite los sitios web:

[https://learn.nsrc.org/bgp/irr\\_objects](https://learn.nsrc.org/bgp/irr_objects)

<https://www.apnic.net/manage-ip/using-whois/guide/as-set/>

Article is closed for comments.



OPEN CONNECT

## Mutually Agreed Norms for Routing Security (MANRS)

Netflix encourages the ISPs we partner with to follow industry best practices in order to build and operate a safer internet. We have adopted Mutually Agreed Norms for Routing Security (MANRS) standards, and we encourage our partners to do the same. MANRS is a global internet safety initiative, supported by the Internet Society.

MANRS standards help the internet community (ISPs, CDNs, and IXs) reduce the most common routing threats, which helps ensure the stability and security of the entire internet ecosystem.

For more information about MANRS, see the information on their [website](#).

Article is closed for comments.



OPEN CONNECT

## RPKI-based route filtering

- Beginning on February 24, 2020, Netflix enabled RPKI filtering on BGP sessions to embedded Open Connect Appliances (OCAs)
- Beginning on September 2, 2020, Netflix enabled RPKI filtering on all peering and transit BGP sessions

Resource Public Key Infrastructure (RPKI) provides a method for networks who have been assigned IP addresses to specify which ASNs are authorized to originate those IP address prefixes via route origin authorizations (ROAs), which are stored and distributed by the regional Internet registries.

By implementing RPKI-based filtering, Netflix is honoring the wishes of ISPs who have chosen to opt into the RPKI ecosystem to protect their IP address space. For ISPs who have not signed their address space, there is no impact.

If you want to check your embedded route announcements to ensure that your ROAs match the routes that Netflix is receiving, you can do so by running a **Route Optimizer report** in the Partner Portal.

**Note:** The **Route Optimizer** report currently does not identify filtered routes that are announced on peering or transit sessions.

Because RPKI-based filtering is being deployed by an increasingly large number of network operators and internet exchange points, the value of signing your address space continues to increase. If you have not yet signed your address space, we recommend that you consider doing so.

For more information about RPKI, see these additional resources:

- <https://www.arin.net/resources/manage/rpki/>
- <https://www.ripe.net/manage-ips-and-asns/resource-management/certification/what-is-rpki>
- <https://www.lacnic.net/1150/1/lacnic/rpki-faq>

Article is closed for comments.



OPEN CONNECT

## Moving an OCA

In some cases, it might be necessary to physically or logically relocate an OCA from one embedded site to another. If you need to move an OCA, you must open a ticket to notify the Open Connect team, so that we can coordinate any necessary configuration changes.

For more details on why these changes are necessary, see the following articles:

- The [Network configuration](#) article explains how content is stored on OCAs within a site, how OCAs are configured into clusters that improve overall offload, and how moving an OCA without properly reconfiguring it can cause problematic traffic patterns.
- The [naming convention](#) article explains how OCAs are identified and named.

### Notes:

- After the OCA has been moved and reconfigured, it will be assigned a new hostname as described in the naming convention article.
- During the configuration change, the OCA will stop serving traffic. After the configuration change, the OCA may not start serving traffic again until after the next fill window.
- In terms of metrics and data, the moved OCA will be treated as a new OCA. It will not retain any historical metrics or audit log history.
- Any tickets that were associated with the OCA before it was relocated will still be associated after the move, however the old hostname might be referenced in earlier ticket comments.

To notify the Open Connect team about an OCA move:

1. [Open a ticket](#), and select the following options:

- **Type:** Partner Request
- **Category:** Moving an OCA
- **Issue:** Relocate OCA to New Site

Type\*

Partner Request

Category\*

Moving an OCA

Issue\*

Relocate OCA to new site

2. Select relevant associated sites and appliances, fill in other fields appropriately, then click **Create**.

An Open Connect team member will respond in the ticket to assist you with next steps.

Article is closed for comments.



OPEN CONNECT

## Fill patterns

Each Open Connect Appliance (OCA) stores a portion of the Netflix catalog, which in general is less than the complete content library for a given region. Popularity changes, new titles that are added to the service, re-encoded movies, and routine software enhancements are all part of the nightly updates, or *fill*, that each appliance must download to remain current.

### FILL WINDOWS

By design, OCAs follow a “push fill” methodology. They primarily fill every day during a window of time that corresponds to your off-peak hours. The timing of the fill window is defined in partnership with your network planning team.

The goal is to set the fill window such that:

- It occurs during the trough of your Netflix traffic
- It does not disrupt your inbound traffic peaks

Setting the fill window this way allows the system to continue to download updates and serve clients without negatively impacting playback performance.

Requirements for the fill window, by hardware type:

Setting	Storage	Global	Flash
Length of time	<b>12 hours</b>	<b>12 hours</b>	<b>12 hours</b>
Timeframe	<b>2AM to 2PM (local time)</b> (can be shifted +/- 2 hours)*	<b>2AM to 2PM (local time)</b> (can be shifted +/- 2 hours)*	<b>2AM to 2PM (local time)</b> (can be shifted +/- 2 hours)*
Bandwidth	Maximum rate of <b>1.2 Gbps per appliance</b>	Maximum rate of <b>0.4 Gbps per appliance</b>	Maximum rate of <b>0.3 Gbps per appliance</b>
Total traffic during fill window	Up to <b>6.5 TB</b>	Up to <b>2.1 TB</b>	Up to <b>1.6 TB</b>

\*All OCAs within a site must begin filling at the same time.

The system might complete filling before the end of the fill window, and it might fill more than once if new content becomes available before the fill window ends.

Most flash-based appliances can fill and serve simultaneously, but some older hardware revisions cannot. These older revisions are configured to fill as much as possible from the storage appliances that are on site, and Netflix traffic is served by the storage appliances on site during their fill period.

For more information about changes to fill patterns that were made after October 2020, see **Media-aware content placement**

## FILL PATTERNS

In general, appliances determine where to receive fill using selection criteria that is similar to **the steering criteria that is used by Netflix client devices**. The following scenarios provide more detail.

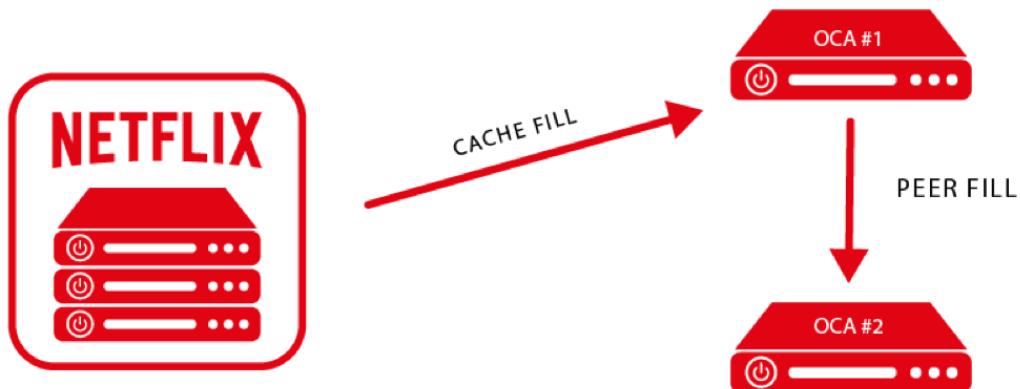
If you have specific fill requirements, discuss them with your partner engagement manager during the initial site design process. If you require changes to your appliance's fill behavior post-deployment, **open a ticket**.

### PEER FILLING

OCAs will attempt to peer fill from each other in either of these two cases:

- If they are clustered
- If they are on the same subnet

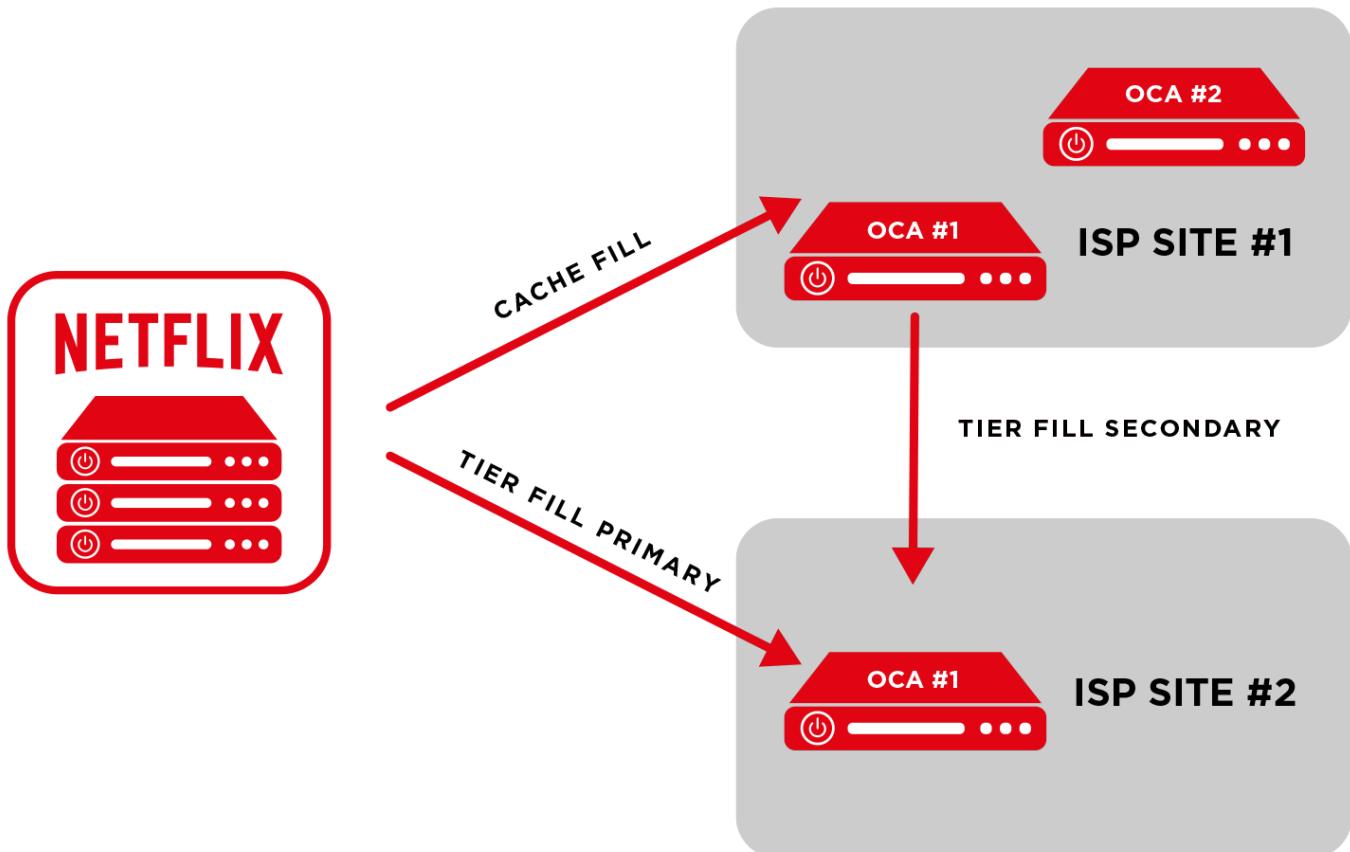
For example, assume that in the following diagram, OCA #1 and OCA #2 are in a cluster. If OCA #1 downloads a movie via a regular cache fill, OCA #2 will then seek to download the movie from OCA #1 instead of via transit or Open Connect peering. Routes to the OCAs must be advertised over Open Connect peering to ensure that the peering session is used for fill traffic.



### TIER FILLING

Peer filling is the most efficient method, however as a second-best option tier filling is considered. OCAs that can see each other's IP address in their BGP feed (but are not in the same cluster or subnet) will consider filling from each other rather than via a regular cache fill.

To identify tier fill issues within your network, you can run the **Tier Fill** report in the [Partner Portal Route Explorer](#) tool.



## OUT-OF-CYCLE FILLS

There will be cases that cause a need to deploy or update a small subset of titles on the OCAs outside of the normal fill window. This need can arise for various reasons, for example:

- If re-encoding of a popular title is required to repair viewing issues
- To make a new, “day-of-broadcast”, or “day-after-broadcast” title available

When these out-of-cycle fills occur, you will see a small portion of fill traffic for a limited period of time outside of the configured fill window. Doing an out-of-cycle fill instead of waiting until the normal fill window helps to ensure that popular titles can continue to be served from your OCAs (the preferred method) and not via peering or transit. This approach improves the overall efficiency and offload potential of the system. Because out-of-cycle fills are limited to very specific popular titles, they do not negatively impact overall server efficiency - rather, they increase the local offload of popular content.

See also: [This blog post about fill](#)

Article is closed for comments.



OPEN CONNECT

## Automatic Software Updates

Netflix manages the OCA software, and we will periodically update or enhance the software. All non-emergency software updates are performed during the configured fill window, and you will be notified when the update starts and after it is complete. All appliance software, including the operating system, web server, and control code, is updated as a single image.

If a new image fails to properly load, the appliance will automatically fall back to the previous image. In most cases, any issues that occur can be resolved on our end and there is no partner action required. If an upgrade fails and we need help resolving the issue, we will open a ticket to your organization.

Article is closed for comments.



OPEN CONNECT

## Health Monitoring

As part of the Open Connect program, Netflix continuously monitors all deployed Netflix OCAs, including all aspects of the performance and availability of the appliance.

For more information on the set of checks that we periodically run on Live and serving OCAs, see: [OCA Live checks](#)

You can monitor the basic health of the OCAs that are deployed on your network by using the Netflix Partner Portal at <https://my.oc.netflix.com>. You will be invited to create an account in the Partner Portal as part of the OCA installation and turn-up process.

For more information about the Partner Portal, see: [Getting started with Partner Portal](#)

Article is closed for comments.



OPEN CONNECT

## OCA Maintenance Policies

- Partner Maintenance
- Unplanned Outages or Service-Impacting Events
- Potential Service-impacting Maintenance

### PARTNER MAINTENANCE

The only OCA components that Netflix will request partners to replace in the field are:

- Power supplies
- Optics

We will ship these components to you in case of failure. Netflix will not request any ISP partner to install or replace any internal OCA hardware components such as memory, hard drives, or fans. Note that OCAs are designed to operate in data center environments with high-capacity fans that are required to cool the dense disk and memory installed. You might notice loud fan noise from OCAs, which is normal.

For ISP partners who are engaging in maintenance that might impact Netflix OCA availability, please observe the following guidelines:

- Plan your maintenance or downtime to occur during the scheduled fill window in order to minimize service disruption to our shared subscribers.
- You can disable and drain appliances from the Open Connect Partner Portal following these instructions: [Draining and disabling appliances](#)
- You can also use the Partner Portal to schedule maintenance in advance.
- Plan to drain appliances of traffic 2 to 3 hours in advance of disconnecting or powering down appliances, so that clients currently being served by the appliance will finish by the start of the maintenance period and new client playback requests are properly directed to an alternate source. This helps to ensure that clients do not need to switch away to a different source mid-stream, which can cause viewing disruptions.
- After completion of maintenance, ensure that the OCAs are re-enabled to serve traffic. This will redirect new session starts away from the alternate sources.
- If you intend to make any physical changes to a site that contains multiple OCAs in a cluster (physically moving OCAs, etc), you must notify the Open Connect team so that the cluster can be reconfigured properly. For more details, see: [Moving an OCA](#)

### UNPLANNED OUTAGES OR SERVICE-IMPACTING EVENTS

For service-wide outages with broad impact to the service of multiple OCA partners, partners might receive an initial notification, status updates on a regular basis if the outage is prolonged, and a final resolution notification. If you want to filter these announcements, the sender address is: cdn-noc@mailer.netflix.com.

For per-ISP partner incidents, including routing and connectivity anomalies that persist over a significant period of time, the Netflix operations team will be alerted by our internal monitoring tools. We will resolve any issues under our control as soon as reasonably possible. If there is an issue that requires partner assistance, we will open a ticket to you.

## POTENTIAL SERVICE-IMPACTING MAINTENANCE

Whenever possible, for any planned maintenance or activity that might adversely impact an OCA or the services that it provides, Netflix will communicate according to the following schedule:

1. Netflix will send an email at the start of any maintenance activity.
2. Netflix will send another email when the maintenance activity is completed, to signal the return to a normal operational state.

For emergency service activities that do not permit our standard advance period, we will notify as early as possible.

During scheduled and emergency Netflix maintenance windows, ISP partners might see their BGP session flap, notice a link-state change with their cache-connected interfaces, and see traffic served from the appliance decrease or go to zero. All of these events are expected.

Under normal conditions, software updates that are not service-impacting will occur during the fill window at a time of low traffic, thereby minimizing potential user impact.

Article is closed for comments.