Nokia express peering

Automate peering engineering to improve the customer experience

Application note
Abstract

If you provide access to content on the internet, it’s crucial to deliver an exceptional customer experience. Consistent high performance is a nonnegotiable requirement, especially to meet the increasing demands of high-bandwidth and low-latency applications such as video streaming and online gaming.

Peering and transit network interconnections play an essential role in providing the performance you require and your customers demand.

This application note explains how Nokia express peering solves the challenges of optimizing peering and transit interconnections by automating peering engineering – to deliver the content and quality of experience your customers demand. We also provide use cases for ingress and egress peer and route optimization.
## Abstract

2

## Your peering and transit challenges – and a solution

4

- Challenges in optimizing peering and transit interconnection
  4
- The Nokia express peering solution
  4
- Peering engineering
  5

## Automated peering engineering

5

## Unique insights and supported technologies

6

- Unique insights applied across all use cases
  6
- Standard technologies supported
  7

## Ingress peer and route optimization use cases

8

- Influencing BGP peering: Ingress peer optimization techniques used for automation
  11
- Preserving common practices using existing BGP standards, behavior and deployment
  11
- Balanced ingress peer and route optimization
  13

## Egress peer and route optimization use cases

14

- BGP AS path optimization
  14
- Latency-based steering optimization
  15
- Congestion-based traffic flow control
  15

## Conclusion

16

## Abbreviations

16
Your peering and transit challenges – and a solution

If you are a service provider, enterprise or webscale company that provides access to content on the internet, it’s crucial to deliver an exceptional customer experience. Consistent high performance and low latency are nonnegotiable requirements, especially to meet the increasing demands of high-bandwidth and real-time applications such as video streaming and online gaming.

Peering and transit network interconnections play an essential role in providing the performance you require – and your customers demand – as well as reducing your costs and simplifying operations.

Challenges in optimizing peering and transit interconnection

Optimizing peering and transit interconnection comes with three main challenges:

• **Routing mechanisms:** It is important to be able to leverage existing infrastructure and routing protocols, but also to be able to overcome their limitations. The Border Gateway Protocol (BGP) inherently lacks information on real-time traffic utilization and performance visibility across various paths. These limitations make it difficult for peering to work effectively on the wide range of today’s traffic. Especially due to cumbersome manual processes and tools, costly mistakes in BGP configuration have led to routing leaks – with serious external impacts such as widespread internet or service outages.

• **Traffic visibility:** Understanding how each application performs across all parts of the network is critical to quickly identify where to move traffic most efficiently and to proactively avoid problems. This requires granular visibility into traffic flows. End-to-end visibility into the complete service delivery path, from content source to endpoint, is also critical to ensure the best performance.

• **People and tools:** Comprehensive solutions and automated processes are required to achieve optimal performance. Network appliances and analytics tools used to measure latency and packet loss measure only from a single peering router to the destination, making their findings incomplete. Today’s tools also do not provide visibility into how specific applications perform across all parts of the network. In addition, shifting live traffic in real time to a less congested link is difficult to achieve using manual processes – and can lead to serious, even catastrophic, events when mistakes are made.

The Nokia express peering solution

Nokia express peering addresses all of your peering and transit challenges. Our solution automates network engineering and mitigates Distributed Denial of Service (DDoS) attacks to enhance the performance of your peering edge through a fundamentally different approach. Nokia express peering leverages insight-driven automated networking (see Figure 1) with:

• Nokia Deepfield analytics for enabling real-time traffic visibility into cloud apps
• The Nokia Network Services Platform (NSP) for instant network resource control and traffic optimization
• Flexibility of choice for a scalable and programmable network fabric that best fits your network engineering and operations.

---

1 For more information about the challenges in optimizing peering and transit interconnection, read the Nokia white paper "Automated peering engineering: Peering optimization in a modern internet world"
Peering engineering

This application note focuses on the peering engineering aspect of Nokia express peering. We describe how customer quality of experience (QoE) can be significantly improved by using automated peering engineering. We outline several use cases that show how automated peering engineering can move traffic flows from congested peering links to lighter-loaded links – or select end-to-end paths that meet the required performance level. For example, during peaks of traffic, this automation can proactively anticipate problems and quickly act to help deliver a flawless video experience by reducing link congestion, packet loss and traffic interruption. Automation can also alleviate possible latency issues for time-sensitive applications such as gaming.

Automated peering engineering

Automating peering engineering addresses the various use cases discussed later in this application note for optimizing egress traffic, ingress traffic, or both. The use cases include standards-based approaches for egress peering engineering (EPE) with many value-added extensions as well as innovations for ingress peering engineering.

The limitation of many existing peering engineering tools today is a limited network scope or a sole focus at only the peering edge. In many cases, optimizing traffic only at the peering edge is not enough. This is why Nokia automated peering engineering was designed with a broader network scope that takes the transport network and/or adjacent networks into account in addition to the peering points; this is the only way to guarantee the best performance end to end.

Visibility and control at only the peering edge allows for selecting the best path between border routers and peers. As shown in Figure 2, with visibility at only the peering edge, it may look like the red dotted line path provides the best performance. However, complete visibility reveals that the gray solid line path is actually the best option. Visibility and control of the entire domain allows for selecting the best path between the edge point where traffic enters into the network, all the way through the network to the border routers and peers.
A limitation of many solutions today is that they require extensive systems integration, programming and custom workflow design before being able to deliver value for peering engineers. The Nokia express peering solution comes ready to use by peering engineers, with intuitive user interfaces for key use cases.

Advanced customization and programmability is also available to increase automation and allow for the best fit into the peering environment. This includes an abstracted approach that allows for integration with existing northbound portals or software tools, and key performance indicator (KPI) data feeds from existing performance collection appliances.

A large set of attributes can be used to derive insights, to determine when and where traffic flows should be steered. These attributes help support sophisticated use cases with fine-grained optimization. They can be used to define intent or they can be used in the closed loop to dynamically program and optimize the network infrastructure and achieve the best outcomes.

Unique insights and supported technologies

This section discusses the criteria for flow classification used for insights along with the standard technologies and protocols that are supported.

**Unique insights applied across all use cases**

The following flow classification criteria can serve as a checklist when evaluating the required attributes of an automated peering engineering solution.
Flow classification, such as 5-tuple, Prefix, autonomous system number (ASN), BGP Community and Differentiated Services Code Point (DSCP), are the most common attributes used to trigger traffic steering. However, the Nokia express peering solution goes beyond these to provide unique insights through more meaningful attributes that are associated with business goals and are easier to manipulate. These attributes include:

- **Cost**: transit fees – This option can, for example, ensure that a transit provider that charges fees is used only when the utilization on direct peering links reaches a certain threshold.

- **Performance**: link utilization, latency, jitter, packet loss – For example, traffic can be moved from an interface before it reaches 80 percent utilization to avoid congestion and service degradation. Time-sensitive applications such as gaming or VoIP can be moved to paths with the lowest end-to-end latency.

- **Geographical coverage**: countries, regions, sites – For example, traffic can avoid paths that traverse certain geographical areas due to a lack of reliability or for security or geopolitical reasons.

- **Source and destination**: enterprises, peering partners, transit providers, content delivery network (CDN) operators and internet exchange providers – For example, lowest latency paths can be favored for financial firms with high-frequency trading.

- **Application type**: video, gaming, storage, VoIP, peer-to-peer, etc. – Application-type granularity is achieved using Nokia Deepfield to perform multidimensional analytics. Peering engineers can select any traffic dimension specified by the Deepfield Cloud Genome dimensioning system to determine traffic steering. With Deepfield cloud application classification enabled, peering engineers can then gain superior visibility into peering prefixes through Deepfield clustering and display of prefixes based on application groups down to the server/domain name server level of granularity. This enables more selective traffic steering and optimization for specific cloud applications.

### Standard technologies supported

Nokia Express peering supports the following standard technologies and protocols:

- Segment routing and RSVP-TE for transport to alternate peering routers
- IPFIX for the exchange of IP traffic flow information and its export
- BGP-LS for topology discovery and for learning peer exit information (e.g., label)
- BGP-LU for route injection
- BGP FlowSpec or OpenFlow for flow rule injection, including BGP route injection
- BMP to enable monitoring through tracking meaningful BGP prefix, policy and KPI changes.
Ingress peer and route optimization use cases

Ingress route optimization enables automatic monitoring of links for high utilization. It then identifies the top traffic consumers by BGP prefixes, destination autonomous system (AS) networks, BGP communities or even per site. Depending on the desired mode of operation – automatic or manual – optimization injects the appropriate BGP policies to shift ingress traffic to selected peers.

Nokia automated peering engineering supports the ability to implement multiple BGP operational models that match either specific or generic existing operational models. This allows for a high level of customization while at the same time supporting the most generic common models so that peering engineers can derive immediate value from automation.

The approach is based on two constructs that are set during initialization of the system; these specify the type of inbound peering model and steering template to be used (see Figure 3).

**Figure 3. Ingress peer optimization: Operational models**

The inbound peering model defines where the automation will be performed. Two settings are supported. “Peering Only” means only external peering. “Extended Peering” means that optimization should operate simultaneously on internal BGP links (from the peering router) and on external peering.

The Steering Template defines two modes of BGP operation: fully automatic mode and manual mode. In fully automatic mode, the system detects congestion and automatically load balances the traffic to the links that have enough bandwidth. The system also determines which BGP policies to inject. In manual mode, the system abstracts the policies but also allows injection of custom BGP policies.

Site and slice constructs are used to provide abstracted-level visibility. Peering engineers find the simplicity of site and slice constructs useful for flexible decision-making about where the ingress peer optimization should be used and where specifically the automation algorithm should operate (see Figure 4).
All necessary information required to make informed traffic steering decisions is considered by the automation algorithm, including important business-intent and routing policy constraints. For example, information on top AS network peers contributing to congestion for ingress traffic is used to provide topology visualization and details on:

- Which specific interfaces are impacted
- How much traffic is flowing on each interface (i.e., for utilization on aggregate or filtered on other specific criteria, such as application type when Nokia Deepfield analytics is integrated)
- Where the traffic is coming from (i.e., which specific peers and which specific BGP prefixes or even filtered down to which domain name server or CDN or content source when Nokia Deepfield analytics is integrated).

In Figure 5, we see for a selected peering AS that is contributing to congestion how advanced visibility is used to inform steering decisions. A complete understanding of all traffic steering options is shown for all alternate paths available.

In this case, three available alternate routes are listed that the engineer can select from to steer traffic. Most important, before taking action the engineer can gain visibility into the impact of the change through a projection that shows the impact of the planned change (i.e., changes to utilization levels) if this action were to be deployed. This makes it easy to understand utilization levels to make the right changes that avoid congestion without guessing or using trial-and-error approaches.
In addition, to provide more intelligence and granular control into automation, links can be tagged with business-level intents or routing policy. For example, links can be tagged to make the automation algorithm consider constraints for an objective of selecting lowest cost links or lowest latency links (see Figure 6, left side).

An advanced feature of this algorithm provides hierarchical automation that injects scope and priority to determine where the automation needs to happen. This granular level of control is especially important for peering engineers working collaboratively with others where there is a division of responsibilities. To meet these needs, the algorithm has been designed to allow automation to be applied in a focused way – for example, to a specific router or a group of routers from a specific site/region or tied to a specific VPN/VRF or network resource optimization slice.

Automation can also be applied across various slices. The priority of the scope of automation and sequence of execution is also controlled by the algorithm (see Figure 6, right side).

**Figure 5. Ingress peer optimization – Slice selection based on utilization**

**Figure 6. Ingress peer optimization – automation algorithm scope and priority**
Influencing BGP peering: Ingress peer optimization techniques used for automation

Automation for ingress peer optimization leverages some of the most popular BGP mechanisms to influence incoming peering traffic from external AS networks. The following sections describe examples of ingress peer optimization techniques used for automation.

Perform AS prepending to routes advertised through undesired interfaces

AS prepending is a popular method used at the BGP routing level to de-prioritize a route by adding the AS number multiple times on the least-preferred route. Because BGP performs routing based on the lowest number of AS networks traversed, it would tend to prefer other routes.

Change BGP Multi Exit Discriminator (MED) parameters

BGP MED is a parameter an ISP uses to signal to the neighboring ISP which interface it prefers for incoming traffic. While AS prepending affects routing beyond the immediate neighboring peering provider, the MED parameters are not transferred beyond the immediate neighbors, and they are often ignored by neighbors unless the two ISPs have a specific agreement.

Tag routes with BGP communities

Some providers have a set of BGP communities that can be used for their peer to manipulate routes that traverse the provider network. The BGP communities are simply values that can be given to certain routes and which will cause specific actions to be taken by the peering provider; for example, assigning higher priority to these routes. This mechanism is often preferred by transit providers because it gives them full control over routing in their network, so they can decide how to handle the request.

Use route injection to advertise a more specific route to the preferred peering provider

Using route injection to advertise a more specific route to the preferred peering provider could increase the number of prefixes (routes) in the internet routing tables. For this reason, it may be undesirable for the wider internet community. This technique also requires the BGP Monitoring Protocol (BMP) to redirect traffic if the route disappears. For both of these reasons, this mechanism is often not used.

Filter on specific prefixes or AS paths

Filtering on specific prefixes or AS paths can be performed to permit or deny known prefixes on ingress traffic for a peer edge router or service edge router (i.e., per customer or per application). This practice is more common on service edge routers in combination with path selection for ingress traffic. For transit scenarios, filtering can be performed to permit or deny specific AS paths.

It is common practice to not create prefix lists for partner AS network peers. However, prefix lists can be created for known subnets to permit known prefixes.

Prefix lists are rarely used to permit prefixes on peering edge routers but are useful to deny prefixes that should not be received. Examples include prefixes from your own AS or for an internet exchange provider, as well as identified DDoS attack threats.

Preserving common practices using existing BGP standards, behavior and deployment

It is important for peering automation to operate in brownfield environments in a way that preserves BGP functions in use without overriding existing behavior. Nokia automated peering engineering not only preserves, but aims to compliment current practices, including leveraging existing BGP standards, behavior and deployment when introducing automation. For example, Nokia automated peering engineering takes network design and implementation for both redundancy and Equal Cost Multipath (ECMP) into account within the automation algorithm (see Figure 7).
In this example, BGP community changes on peering points are to be deployed for moving a community from one peering point to another. The automation algorithm will drop the community from one peering point and add it to the second while enforcing redundancy by using AS prepending to build a sequence of alternate peers ordered by the best alternative (see Figure 7, left side). This sequence of alternate peers functions to protect against failure scenarios as well as against congestion or performance issues that trigger a predefined threshold.

For preserving ECMP, the automation algorithm can use tagging to color peer links (see Figure 7, right side). This coloring is also as previously discussed in Figure 6 and illustrates the difference between using coloring to achieve a routing policy objective in this case, versus business intent objectives such as for selecting lowest cost or lowest latency links.

**Figure 7. Ingress peer optimization – preserving BGP standards, behavior and deployment**

A common practice to isolate a BGP route advertised to different peering partner networks is to use internet tables on virtual private networks/virtual routing and forwarding (VPNs/VRFs) at the peering edge to ensure secure separation for ingress traffic by exporting to a specific VRF per AS network. Nokia’s ingress peer optimization supports this use case by automating the injection of BGP policies that support exporting traffic flows to, or importing traffic flows from, a VPN/VRF (see Figure 8). Multi-homing scenarios are also supported.

**Figure 8. Ingress peer optimization: Export to/import from a VPN/VRF per peer**
Balanced ingress peer and route optimization

Nokia automated peering engineering extends the ingress use case with an option for balanced route optimization. This option enables ingress traffic to be transported across the network on the most optimal path, starting as it enters the network from the ingress peering point.

Balanced ingress peer and route optimization can be as simple as balancing the traffic from ingress peering routers onto internally-facing network interfaces. Balanced ingress route optimization can also be used to determine how to reach the best egress point for the traffic: either towards the end user through a provider edge (PE) or for transit traffic to an autonomous system boundary router (ASBR)/border router and peering link.

The latter use case is achieved through the ability of automated peering engineering to program PEs receiving the ingress traffic with a segment routing label stack. The label stack includes the segment associated with the egress BGP peer link. In this case, the ASBR becomes a service router label switched router (SR LSR) and will forward to the peer based on the segment routing label.

In addition to setting policies for automating label switched path (LSP) and slice selection, a peering engineer can also manually select an SR-TE or RSVP-TE LSP that terminates on an edge router based on traffic insights, such as utilization or latency, and then select specific known prefixes to be permitted (e.g., per customer or per application). This functionality is available to enterprise customers if enabled through a self-service customer portal.

For transporting transit traffic, the most optimal egress exit point is selected automatically based on EPE policies, which are extended to enable unique insights, such as cloud application context, through Nokia Deepfield analytics. For example, insights such as those for utilization can be monitored to ensure proper balancing from internal network resource slices (see Figure 9, left side) to external peers (see Figure 9, right side). Further details on EPE and automation for egress peer and route optimization can be found in the next section of this paper.

Figure 9. Balanced ingress peer and route optimization: Example for internal- to-external utilization
Egress peer and route optimization use cases

Egress peer and route optimization provides a generic framework with which peering engineers can use insight to steer traffic to the most optimal next-hop peer or to an MPLS path (for example, an SR-TE LSP). This use case also leverages EPE standards.

With the full set of unique insights provided by the Nokia solution, the peering engineer can optimize egress routes based on congestion; for example, to steer all CDN traffic, video traffic, per-country traffic or per-application traffic to an alternate peering point or path.

There are various enhanced use cases for egress route optimization that can be used in conjunction with the generic framework to improve the end-user QoE.

**BGP AS path optimization**

For BGP AS path optimization, Nokia automated peering engineering allows peering engineers to shift egress traffic to different egress peering points that are most optimal for the traffic to reach its destination. Automated peering engineering does this based on insights for peering AS networks – whether public, transit or private. For example, BGP AS path optimization could be based on insights into congestion.

Automated peering engineering allows destination-based targeting and redirection of top traffic flows (e.g., per application) by prefix at the egress peering point. Peering engineers are able to gain visibility into the impact of congestion and then select specific traffic flows to steer to an alternate peer.

For example, Figure 10 shows an end-to-end path for specific application traffic from a content provider (AS 1000) to a destination (AS 5000). The full BGP AS path is AS 1000 – AS 2000 – AS 4000 – AS 5000.

The Nokia solution allows optimization policies for any traffic from AS 1000 to a specified BGP AS destination. At the AS 1000 egress peering point, Nokia BGP AS path optimization detects congestion and shifts the traffic flows from AS 2000 to AS 3000 automatically (or when initiated by a peering engineer) to avoid potential performance issues from arising. The BGP AS path becomes AS 1000 – AS 3000 – AS 4000 – AS 5000.

Figure 10. BGP AS path optimization for automating peering engineering
Latency-based steering optimization

For latency-based steering optimization, Nokia automated peering engineering allows peering engineers to leverage automated collection of performance monitoring of external destination addresses from a peering edge router. For this use case, the set of addresses to probe is automatically derived from an external analytics system, such as Nokia Deepfield, deep packet inspection probes and/or performance monitoring probes from the network and appliances. This data enables the selection and automated steering for top prefixes based on latency.

The goal is to select the best exit peering point (a specific ASBR/border router and peering link) that provides the lowest latency to an end destination. Traffic for that destination is then automatically steered inside the network to the selected router through an MPLS path, for example, an SR-TE LSP.

The latency values considered are both those for LSPs internally across the MPLS network as well as the latency values from various peering exit points toward external AS networks facing the end destination (see Figure 11).

This use case can also be extended to integrate and function with external route controllers to make the solution a better fit with the existing peering engineering environment and the provider’s extended capabilities.

Figure 11. Latency steering optimization visibility for automating peering engineering

Congestion-based traffic flow control

To avoid and resolve congestion, traffic flow steering is used to automatically and intelligently detect congestion and steer specific traffic flows according to policies. This is achieved by using BGP FlowSpec or OpenFlow for flow rule injection. Peering engineers may decide, for example, to steer flows for specific VIP applications or customers, or to steer huge “elephant” flows. This traffic can be steered onto a specific VPN service, LSP or interface.
Conclusion

Automating peering engineering with the Nokia express peering solution provides crucial advantages compared to existing approaches available for peering engineering. With new levels of insight, peering engineering can now anticipate and react quickly to sudden changes in traffic patterns. This faster response time reduces congestion and improves performance for dynamic and bandwidth-sensitive applications.

It’s a fundamentally different approach to peering that alleviates inefficiencies by automating the cumbersome, complex manual processes currently used. This approach enables superior visibility into traffic flows through unique insights. These provide peering automation at the level that fits the current peering environment, existing investments and operational practices.

With the Nokia express peering solution, peering engineers now have the level of visibility and control needed to enable exceptional customer experiences with consistently high performance and low latency. The business benefits of improving the customer experience are higher customer retention and new revenues from new customers.

Automating peering engineering also enables you to reduce both OPEX and CAPEX. For example:

- Automated traffic steering enables more efficient use of interfaces, resulting in a reduction of hardware ports at these interfaces.
- Better use of available bandwidth minimizes the need for extra transit capacity.
- Operational procedures are simplified, reducing the pressure on skilled network operations staff and special networking tools.

Finally, automated processes help avoid human errors, including mistakes that cause traffic interruptions, incur cost penalties, and require additional time and resources to isolate and fix issues.

To learn more about this solution, visit the Nokia express peering web page.

Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS</td>
<td>autonomous system</td>
</tr>
<tr>
<td>ASBR</td>
<td>autonomous system border or boundary router (ASBR is also referred to as “border router” or “peering router” in this paper.)</td>
</tr>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
</tr>
<tr>
<td>BGP-LS</td>
<td>BGP – Link State</td>
</tr>
<tr>
<td>BGP-LU</td>
<td>BGP – Labeled Unicast</td>
</tr>
<tr>
<td>BMP</td>
<td>BGP Monitoring Protocol</td>
</tr>
<tr>
<td>CDN</td>
<td>content delivery network</td>
</tr>
<tr>
<td>DSCP</td>
<td>Differentiated Services Code Point</td>
</tr>
<tr>
<td>ECMP</td>
<td>Equal Cost Multipath</td>
</tr>
<tr>
<td>EPE</td>
<td>egress peering engineering</td>
</tr>
</tbody>
</table>
ISP     internet service provider
LSP     label switched path
MED     Multi Exit Discriminator
MPLS    multiprotocol label switching
QoE     quality of experience
RSVP-TE Resource Reservation Protocol – Traffic Engineering
SR-TE   Segment Routing – Traffic Engineering
VoIP    voice over IP
VPN     virtual private network
VRF     virtual routing and forwarding

About Nokia

We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry’s most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in digital health, we are shaping the future of technology to transform the human experience. networks.nokia.com

Nokia operates a policy of ongoing development and has made all reasonable efforts to ensure that the content of this document is adequate and free of material errors and omissions. Nokia assumes no responsibility for any inaccuracies in this document and reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2019 Nokia
Nokia Oyj
Karaportti 3
FI-02610 Espoo, Finland
Tel. +358 (0) 10 44 88 000

Document code: SR1902032282EN (March) CID205996