NOKIA

Nokia Service Routing Certification (SRC) Program

Nokia Network and Service Router Security

TTP30096 - v1.0.1

Nokia
Service
Routing
Certification

1 © 2021 Nokia

SRC Sample Course

Module 0

Service Routing Certification (SRC) Program overview

NOKIA

SRC Sample Course

Module overview

Service Routing Certification (SRC) Program overview

Certifications

Courses

Flexible learning options

Exams scheduling and certification tracking

Validating your accomplishments

NOKIA

Service Routing Certification (SRC) Program Overview

Nokia's flagship IP/MPLS training and certification program

Over 15 courses and workshops

3 industry recognized certifications

Developed by Nokia subject matter experts using industry best practices, use case driven examples, and hands-on labs

Flexible learning options to meet individual learner needs

nokia.com/networks/training/src

Nokia
Service
Routing
Certification

NOKIA

SRC Sample Course

Certifications

Nokia Certified Network Routing Specialist I	Nokia Network Routing Specialist I (NRS I) Certification Learn the essentials of IP networking and VPN service routing Learn more
Nokia Certified Network Routing Specialist II	Nokia Network Routing Specialist II (NRS II) Certification Acquire Nokia IP/MPLS service routing expertise Learn more
Nokia Certified Service Routing Architect	Nokia Service Routing Architect (SRA) Certification Master the knowledge and skills to design and support high performing Nokia Service Router networks Learn more

Certification requirements

Recommended courses/mandatory written exams	Nokia Certified Network Routing Specialist I	Nokia Certified Network Routing Specialist II	Nokia Certified Service Routing Architect
Nokia IP Networks and Services Fundamentals	■		
Nokia IS-IS Routing Protocol		■ *	■ *
Nokia OSPF Routing Protocol		■ *	■ *
Nokia Border Gateway Protocol Fundamentals for Services		■	
Nokia Border Gateway Protocol for Internet Routing			■
Nokia Multiprotocol Label Switching		■	■
Nokia Services Architecture		■	■
Nokia Virtual Private LAN Services			■
Nokia Virtual Private Routed Networks			■
Nokia Quality of Service			■
Recommended courses/mandatory elective exams**			
Nokia Multicast Protocols			■ **
Nokia Network and Service Router Security			■ **
Mandatory Practical Lab Exams			
Nokia NRS II		■	
Nokia SRA			■

* Choose the IS-IS or OSPF Protocol written exam
**Choose the Multicast Protocols or Network and Service Router Security written exam

- Pass all required exams to certify
- Certifications are valid for 3 years
- Recertification exams are required to maintain active certification status

Legend
- Courses/ written exams
- SRA elective written exams
- Practical lab exams

NOKIA

Courses

Course name	Course number	Exam number	Course duration
Nokia IP Networks and Services Fundamentals	3FL30632AAAAZZZZA	4A0-100	4 days
Nokia IS-IS Routing Protocol	OP00060-V-2010	4A0-112	3 days
Nokia OSPF Routing Protocol	OP00061-V-2010	4A0-113	3 days
Nokia Border Gateway Fundamentals for Services	OP00059-V-2010	4A0-114	2 days
Nokia Border Gateway Protocol for Internet Routing	3FL30634AAAAZZZZA	4A0-102	4 days
Nokia Multiprotocol Label Switching	3FL30635AAAAZZZZA	4A0-103	3 days
Nokia Services Architecture	3FL30636AAAAZZZZA	4A0-104	3 days
Nokia Virtual Private LAN Services	3FL30637AAAAZZZZA	4A0-105	5 days
Nokia Virtual Private Routed Networks	3FL30638AAAAZZZZA	4A0-106	4 days
Nokia Quality of Service	3FL30639AAAAZZZZA	4A0-107	5 days
Nokia Multicast Protocols	3FL30640AAAAZZZZA	4A0-108	5 days
Nokia Network and Service Router Security	TTP30096	4A0-111	4 days
Nokia Advanced Troubleshooting	3FL30642AAAAZZZZA	N/A	5 days
Practical lab exams			
Nokia NRS II Lab Exam	N/A	NRSII4A0	N/A
Nokia SRA Lab Exam	N/A	ASRA4A0	N/A

8 © 2021 Nokia Nokia Multicast Protocols - 3FL30640AAAAZZZZA - v4.1.2 NOKIA

Flexible learning options

Courses/workshops

- Instructor-led courses and workshops to prepare for written and lab exams
- Virtual and face-to-face deliveries
- Attend regularly scheduled public classes across multiple time zones
- Schedule private classes virtually, at your office, or at select Nokia facilities

Self-paced learning

- Electronic copies of course materials for self-study, including:
  - Course lecture materials
  - Lecture notes
  - Module summaries
  - Module learning assessments
  - Lab guides
- Free practice exams

MySRLab

- 24/7 remote lab access to a hosted Service Router lab
- Practice your skills and prepare for lab exams
- Complement your self-study course materials

NOKIA

Exam scheduling and certification tracking

Student portal

- One place to track your certification requirements and status and to receive updates
- Schedule and reschedule exams
- Plan a certification path
- Track your certification progress and view exam results
- Renew your certifications

Written exams

- Take exams virtually from your home/office or from 5000+ test sites worldwide
- Multiple choice, requires 80% passing score

Pearson | VUE

OnVUE

Lab exams

- Administered from select Nokia locations worldwide
- A practical hands-on exam that requires an 80% passing score

nokia.com/networks/training/src/exams

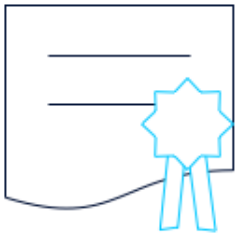
Validating your accomplishments

Digital badges

Receive a digital badge from Credly Acclaim when you pass any exam or become certified

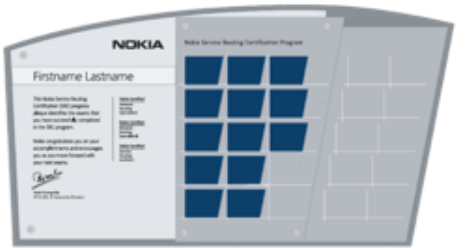
Diploma

Receive a diploma in the mail when you become NRS I, NRS II, and SRA certified



Plaque

Receive a plaque in the mail when you pass any two exams from the SRC program and receive a new tile for each subsequent exam



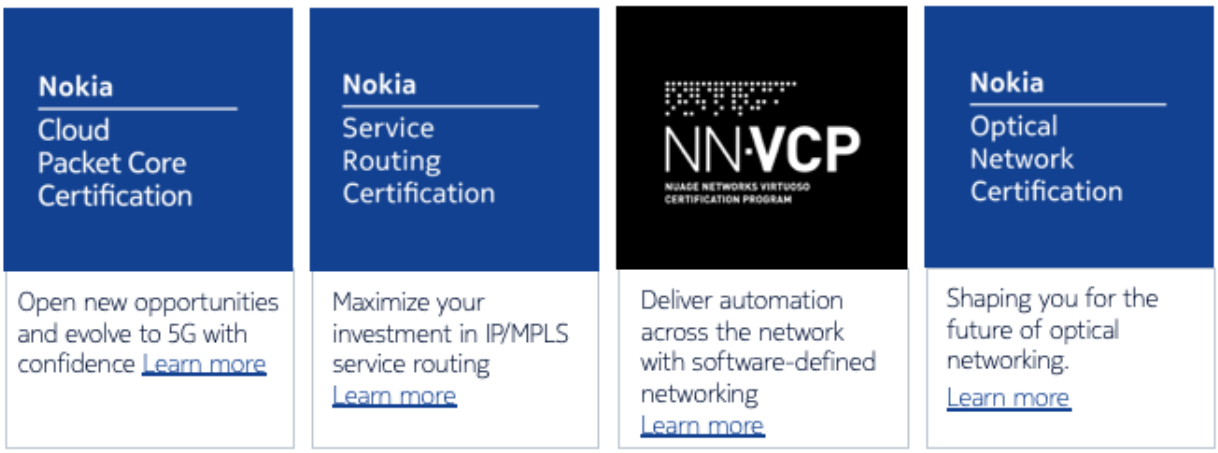
11 © 2021 Nokia

Nokia Multicast Protocols - 3FL30640AAAAZZZZA - v4.1.2

NOKIA

SRC Sample Course

An End-to-End Learning Program



Open new opportunities and evolve to 5G with confidence Learn more

Maximize your investment in IP/MPLS service routing
Learn more

Deliver automation across the network with software-defined networking
Learn more

Shaping you for the future of optical networking.
Learn more

How to purchase

Attend a class

See a global class schedule and register at the following link - nokia.com/networks/training/src/courses

Purchase self-paced learning

To purchase self-paced learning, visit the following link - nokia.com/networks/training/src/self-paced

Register for an exam

To register for an exam and download practice exams, visit - nokia.com/networks/training/src/exams

Questions

For any program-related questions, contact learning.services@nokia.com

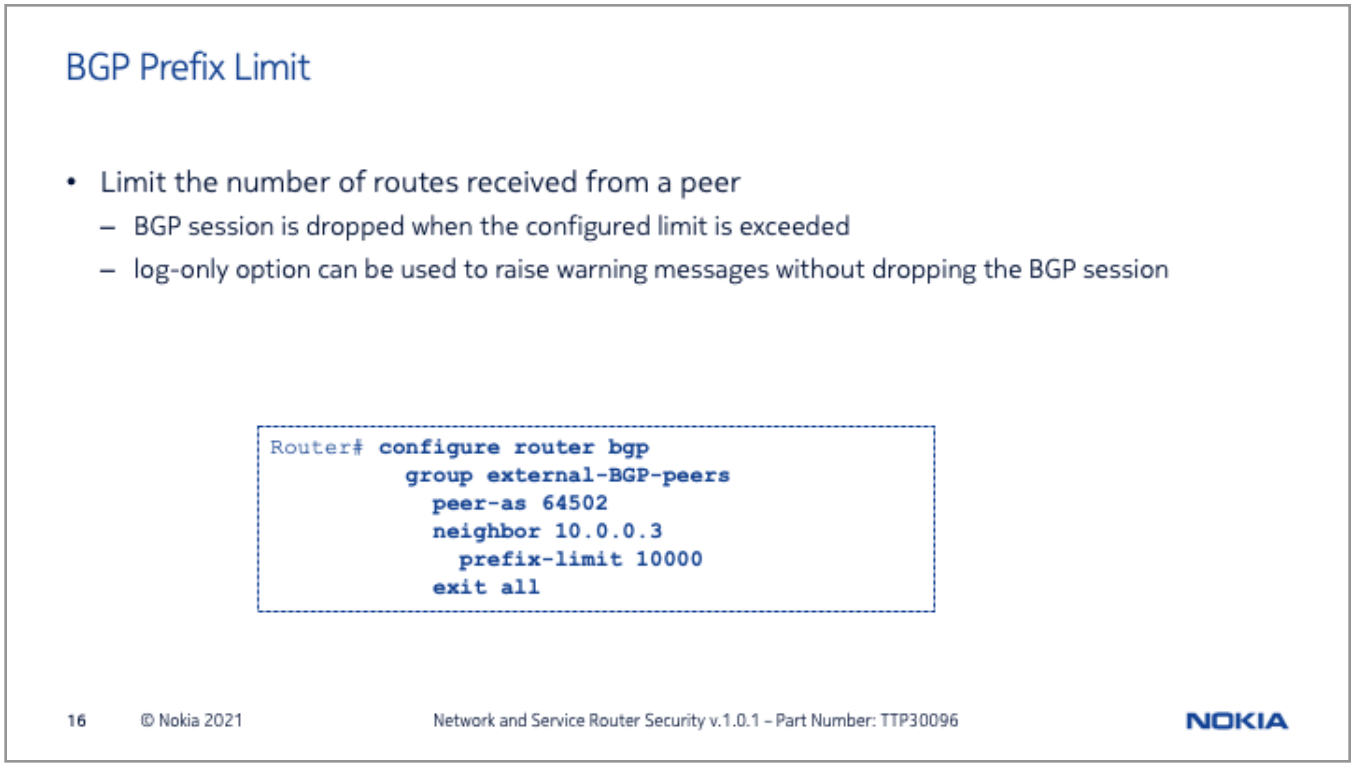
NOKIA

Sample Content

Network and Service Router Security
Course Number: TTP30096
Exam Number: 4A0-111

Course Outline
Network and Service Router Security

- Module 1– Introduction to Security
- Module 2 – SR OS Management Plane Security
- Module 3 – SR OS Control Plane Security
- Module 4 – SR OS Data Plane Security



BGP Prefix Limit

The size of the Internet table is constantly increasing. By default, routes received from external peers are propagated to all internal peers. A high number of routes require significant memory and CPU cycles. To prevent CPU or memory exhaustion, route filters and policies can be deployed to control the set of routes. In addition, a prefix limit can be configured to hard limit the number of routes that can be learned from a peer. When the limit is exceeded, the BGP session is dropped. A threshold percentage can be optionally configured to trigger a warning message/SNMP trap when the threshold is reached. A log-only option can also be configured; in this case a first warning message is sent at the specified threshold and a second one is sent when the limit is exceeded, but the BGP session is not dropped.

BGP Prefix Length Limit

- Restricts prefixes to a specific prefix length n
  - "0.0.0.0/0 through n" matches any prefix with a length less than or equal to n
  - A BGP import policy is configured to accept only prefixes within the specified range

```
Router# configure router policy-options
          begin
          prefix-list "upto-length20"
            prefix 0.0.0.0/0 through 20
          exit
          policy-statement "accept-upto-20"
            entry 10
              from
                prefix-list "upto-length20"
              exit
              action accept
              exit
            exit
            default-action reject
            exit
          exit
          commit
        exit
Router# configure router bgp group eBGP import "accept-upto-20"
```

17 © Nokia 2021 Network and Service Router Security v.1.0.1 – Part Number: TTP30096 NOKIA

BGP Prefix Length Limit

To avoid inflating the route tables and save router resources, a network provider can restrict the prefix length of routes received from an eBGP peer. A BGP import policy can be configured to accept only prefixes with a certain length, and prefixes that are too specific (i.e. have longer length) are simply rejected.

On the Nokia 7750 SR, the prefix "0.0.0.0/0 through 20" matches any prefix with a length less than or equal to 20. An import policy is configured to accept only matching prefixes, and is applied to the eBGP peer. Any incoming BGP routes longer than 20 are rejected.

BGP Route Origin Validation (ROV) – The Need

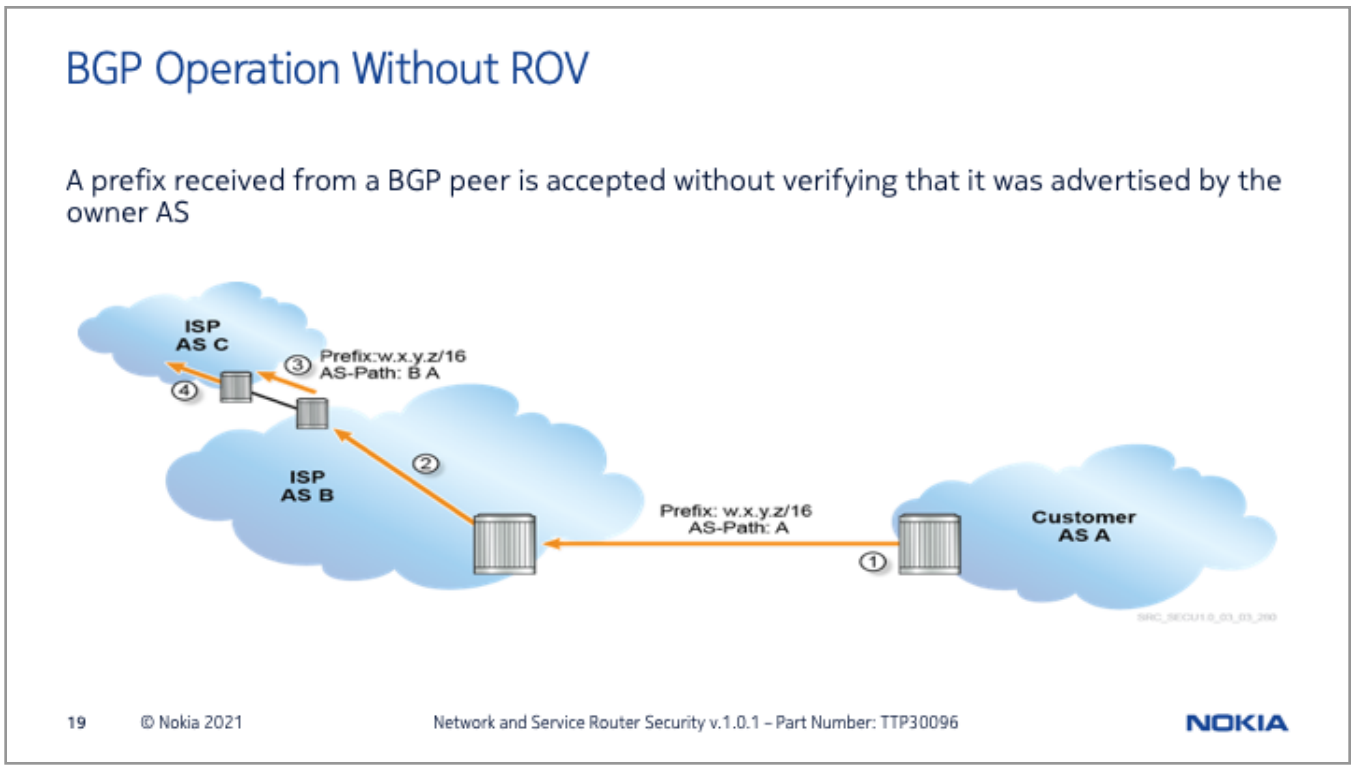
- BGP lacks origin validation
  - An AS can originate any prefix
    - May cause an outage (e.g. YouTube outage in 2008)
- ISPs use policies or filters to reject bad announcements
  - A huge set of filters is required
    - Impacts router performance
  - Filters are not dynamic, hard to keep up-to-date

BGP Route Origin Validation (ROV) – The Need

The Internet architecture relies on trust, and most networks trust each other's route advertisements without validation. When a BGP peer AS originates a prefix, it is assumed that it has the right to announce that prefix. BGP does not validate the origin of a prefix, so any AS can originate any prefix.

Incorrect BGP prefix announcements may cause outages and denial of service. In 2008, a more specific YouTube prefix was accidently advertised by an ISP to its upstream ISPs, instead of being used internally to block YouTube access. The more specific route was advertised globally, and traffic destined for YouTube was forwarded to that ISP because IP routing uses the longest prefix match rule. This caused a YouTube global outage for a couple of hours.

ISPs can use policies or filters to reject bad route advertisements, but there are a few drawbacks with this approach. A huge set of filters will be required to validate the origin of all prefixes, and this impacts the router's performance. In addition, filters are statically configured so it is difficult to keep them up-to-date.

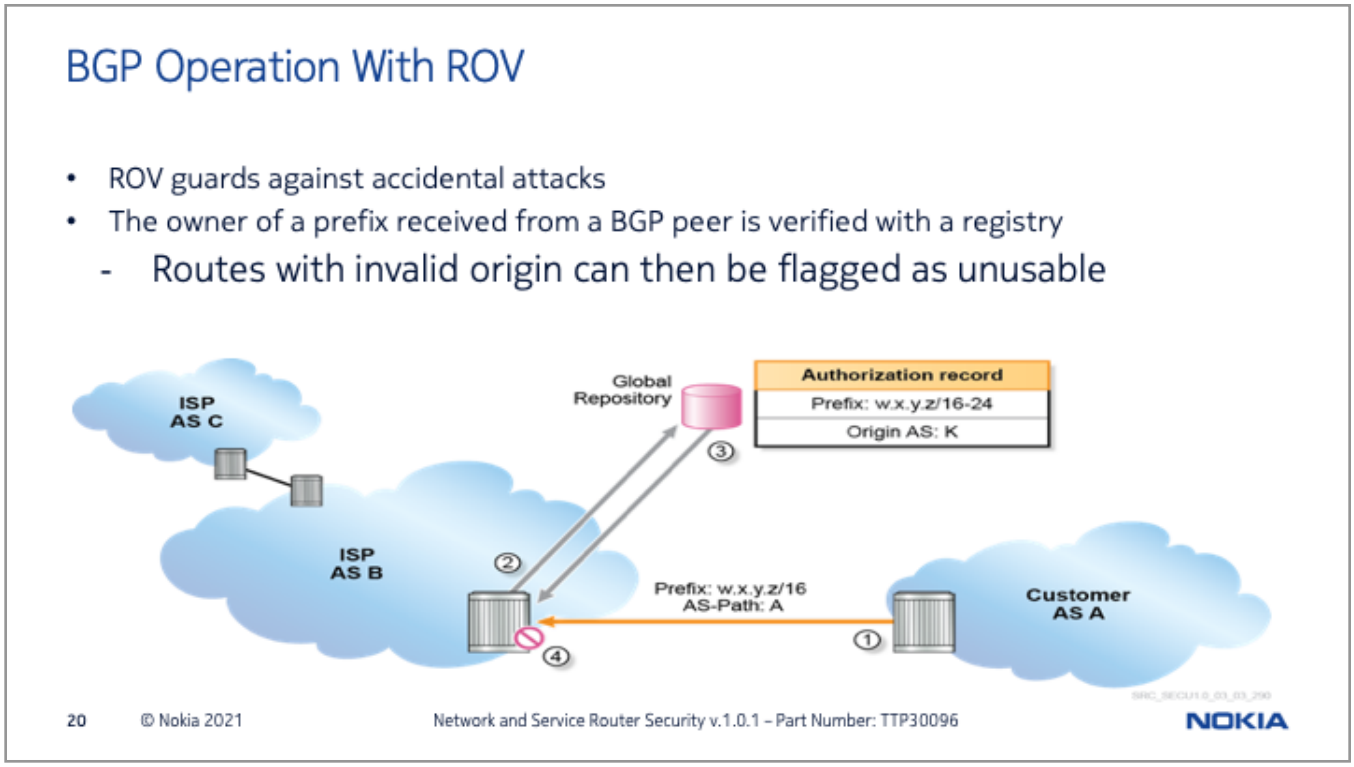


BGP Operation Without ROV

By default, a BGP router accepts a prefix received from its peer without validating that the advertising AS is actually the owner of that prefix. A BGP policy may be used to perform some validation, but this policy needs to be constantly updated.

In the diagram shown in the slide:

1. AS A advertises the prefix w.x.y.z/16 to AS B.
2. The border router of AS B accepts the route and propagates it internally within its AS.
3. AS B advertises the prefix to AS C.
4. The border router of AS C accepts the route and propagates it internally. The prefix is therefore globally advertised.



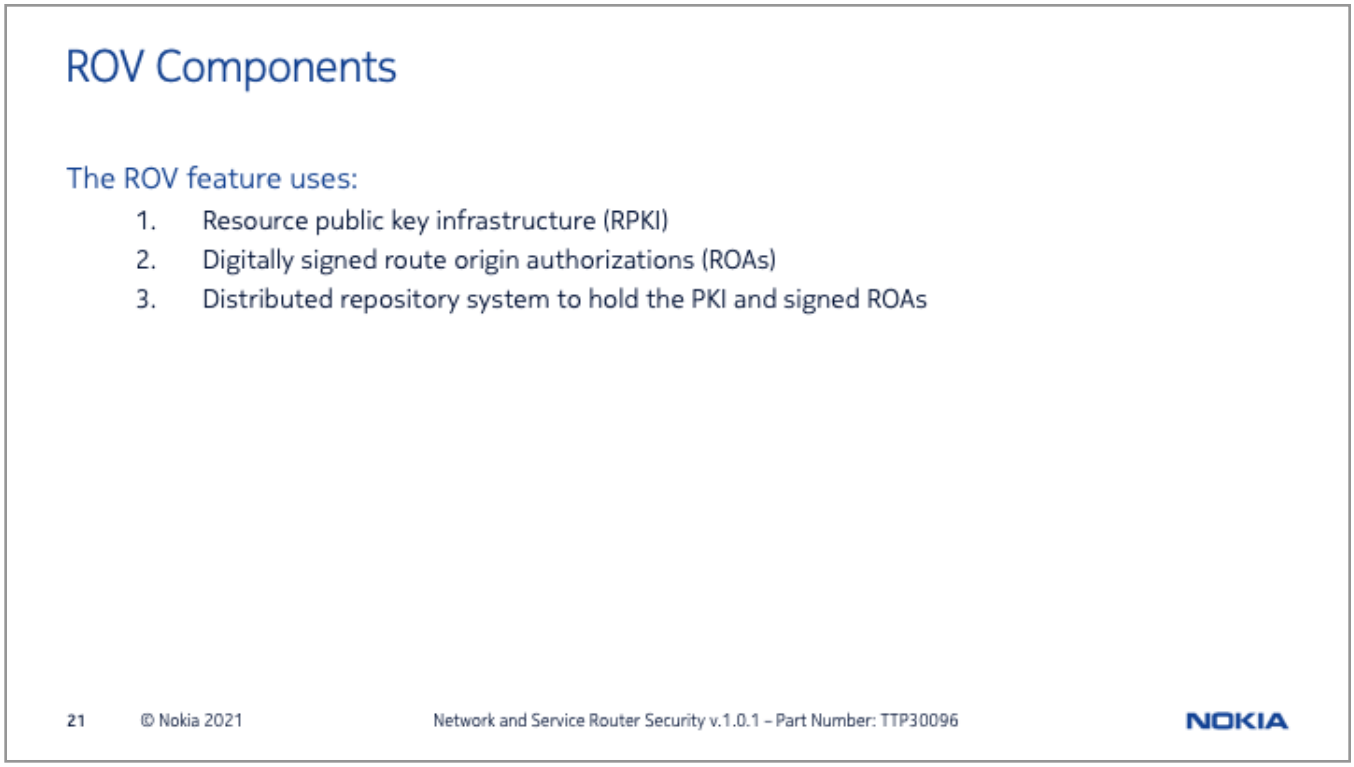
BGP Operation With ROV

When ROV is used, a BGP router first validates that a received BGP route originated from the expected AS before accepting it. If the AS advertising the prefix is the owner, the route is accepted. Otherwise, the route can be flagged as invalid and is not advertised.

ROV guards against accidental attacks or unintentional advertisements where a BGP router advertises a route for a prefix that it does not own but where the AS-Path of that route is not altered. ROV does not protect against targeted attacks where a rogue device intentionally injects a BGP update for a prefix that it does not own and sets the AS-Path as if the route was advertised from the prefix owner. In the latter case, another technique—such as implementing MD5 authentication or ensuring that the first AS in the AS-Path of an incoming route matches the AS number of the eBGP peer— is required on BGP routers to verify the integrity of the BGP update.

In the diagram shown in the slide:

1. AS A advertises the prefix w.x.y.z/16 to AS B.
2. The border router of AS B receives the route and queries a global repository for the prefix owner.
3. The global repository informs the border router that the owner of prefix w.x.y.z/16 is AS K.
4. The border router flags the route as unusable because its origin validation state is invalid (the right-most AS number in the AS-Path attribute indicates that the route is advertised by AS A, which is not the prefix owner).



ROV Components

BGP route origin validation protects against accidental/deliberate prefix hijacking by ensuring that prefixes are advertised by authorized ASes. A legitimate IP prefix owner can authorize one or more ASes to originate routes from its assigned address space. BGP may then consider an IPv4/IPv6 route invalid if it originated from an unauthorized AS, as indicated by the repository.

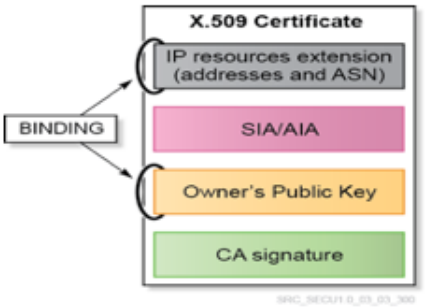
ROV uses a resource public key infrastructure (RPKI) database to verify the owner of a prefix. This distributed database contains cryptographic objects that attest the holding of IP addresses and AS numbers.

A route origin authorization (ROA) is a digitally signed object and attests that an AS is authorized to announce a prefix. The ROA is signed by the owner of the prefix and the attestation is verified cryptographically using RPKI.

A distributed repository system holds the signed ROAs, so that ISPs are able to make BGP route decisions based on available information. A distributed system also protects against a single point of failure in the architecture.

1. Resource PKI (RPKI)

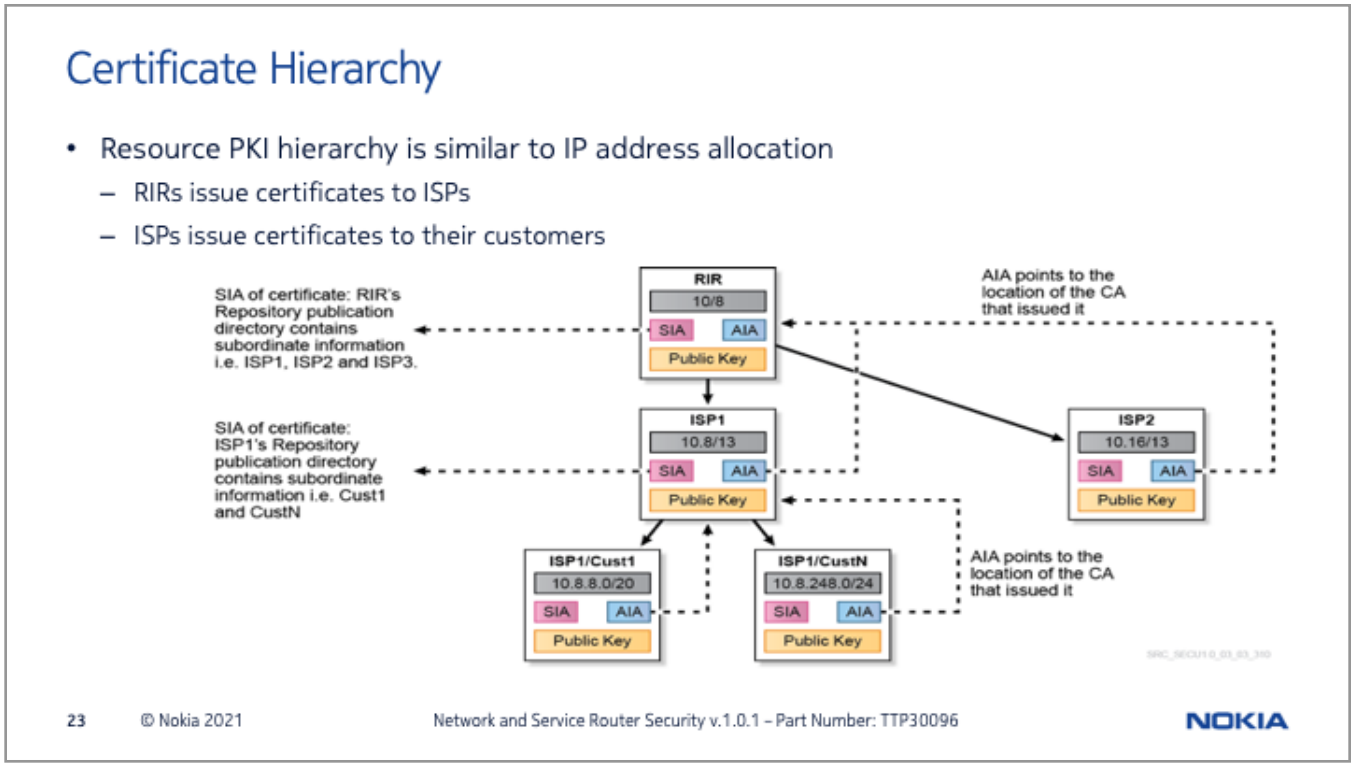
- Cryptographically verifies the IP address allocation to the owner of the address space
- Resource certificate binds
  - IP prefix
  - Public key



Resource PKI (RPKI)

RPKI uses X.509 certificates to bind public keys to a list of IP prefixes or AS numbers. The X.509 extensions defined in RFC 3779, *X.509 Extensions for IP Addresses and AS Identifiers*, are used to specify the list of IP prefixes or AS numbers within the certificates.

The primary function of RPKI is authorization, not authentication. An RPKI certificate binds an IP prefix to a public key, and is signed by the certificate authority (CA) that issued that certificate.



Certificate Hierarchy

The IP address space is managed by a hierarchy rooted at the Internet assigned number authority (IANA). IANA delegates addresses to different regional Internet registries (RIRs). Another level of hierarchy consisting of national Internet registry (NIR) or local Internet Registry (LIR) may also exist. An address holder then receives an IP prefix from one of these registries.

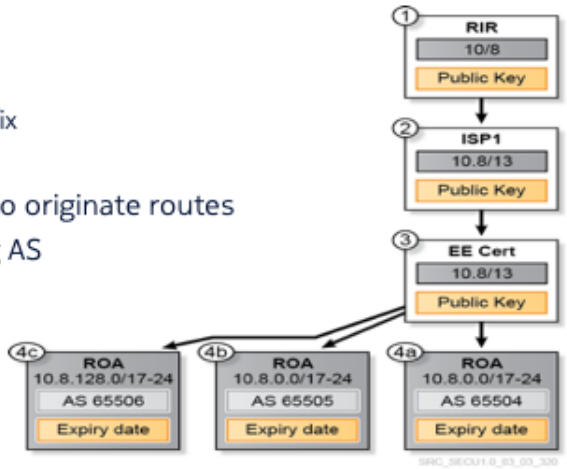
A resource PKI hierarchy is used to verify route origination; certificates are issued following the IP address hierarchy. A self-signed certificate is used as a root certificate, and subordinate certificates are then issued based on the sub-allocation of IP addresses. RIRs assign IP addresses to ISPs and issue certificates to them. Similarly, ISPs assign IP addresses to their customers and issue certificates to them. Each certificate is signed using the private key of the parent certificate authority (CA), and the signature is verified using the public key in the parent certificate.

For every certificate in the PKI, there is a corresponding repository publication point file system directory that is the authoritative publication point for all objects (e.g. certificates, ROAs) verifiable by this certificate. A subject information access (SIA) contains a uniform resource identifier (URI) that references this repository publication point. In the diagram, the SIA of RIR certificate points to a directory containing ISP1 and ISP2 certificates, whereas the SIA of ISP1 certificate points to a directory containing ISP1 customer certificates.

An authority information access (AIA) contains a URI that references the location for the CA certificate under which the given certificate was issued. In the diagram, the AIA of ISP1 and ISP2 certificates point to the RIR certificate, whereas the AIA of ISP1 customer certificates point to the ISP1 certificate.

2. Route Origin Authorization (ROA)

- A digitally signed object that contains:
  - IP prefix
  - Minimum and maximum prefix length
  - AS number allowed to originate routes for the prefix
  - Expiry date
- Issued by the prefix owner to authorize an AS to originate routes
- A separate ROA is required for each advertising AS



Route Origin Authorization (ROA)

An ROA is an attestation that the holder of an IP prefix has authorized an AS to originate routes for that prefix. An ROA contains: an IP prefix with a minimum and a maximum prefix length, an AS that is allowed to originate routes for the prefix, and an expiry date. A resource holder's certificate authority (CA) issues end entity (EE) certificates, which are used to validate the ROAs.

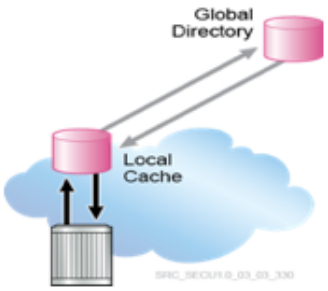
ROAs are required because the IP address allocation information stored in certificates is not sufficient to perform route validation. A prefix owner allows itself and/or other ASes to originate routes for the prefix. Because an ROA contains a single AS, there are as many ROAs as the number of authorized ASes. ROAs are typically stored in repositories that are accessible to all ISPs.

In the diagram shown in the slide:

1. An RIR has a certificate that binds the IP prefix 10.0.0.0/8 with a public key.
2. The RIR assigns the block 10.8.0.0/13 to ISP1 and issues a certificate for it.
3. Assuming ISP1 has only a single customer that gets this IP prefix, this customer generates an EE certificate for its assigned prefix.
4. The customer then creates ROAs based on its advertisement needs and signs them using its EE certificate:
   a. An ROA is signed for AS 65504 to advertise the block 10.8.0.0/17-24.
   b. For redundancy purposes (dual homing), a second ROA is signed for AS 65505 to advertise the same block 10.8.0.0/17-24.
   c. A third ROA is signed for AS 65506 to advertise the block 10.8.128.0/17-24.

3. Distributed Repository

- Global Directory
  - Distributed among RIRs
  - Holds ROAs and certificates
  - Certificates are issued only by resource holders
  - Database records are manipulated only by authorized resources
- Local cache
  - Queries the global directory for a copy of all certificates
  - Verifies the signature of each certificate
  - Validates the certification path of EE certificates
  - Updates its database periodically
  - May contain static and dynamic entries



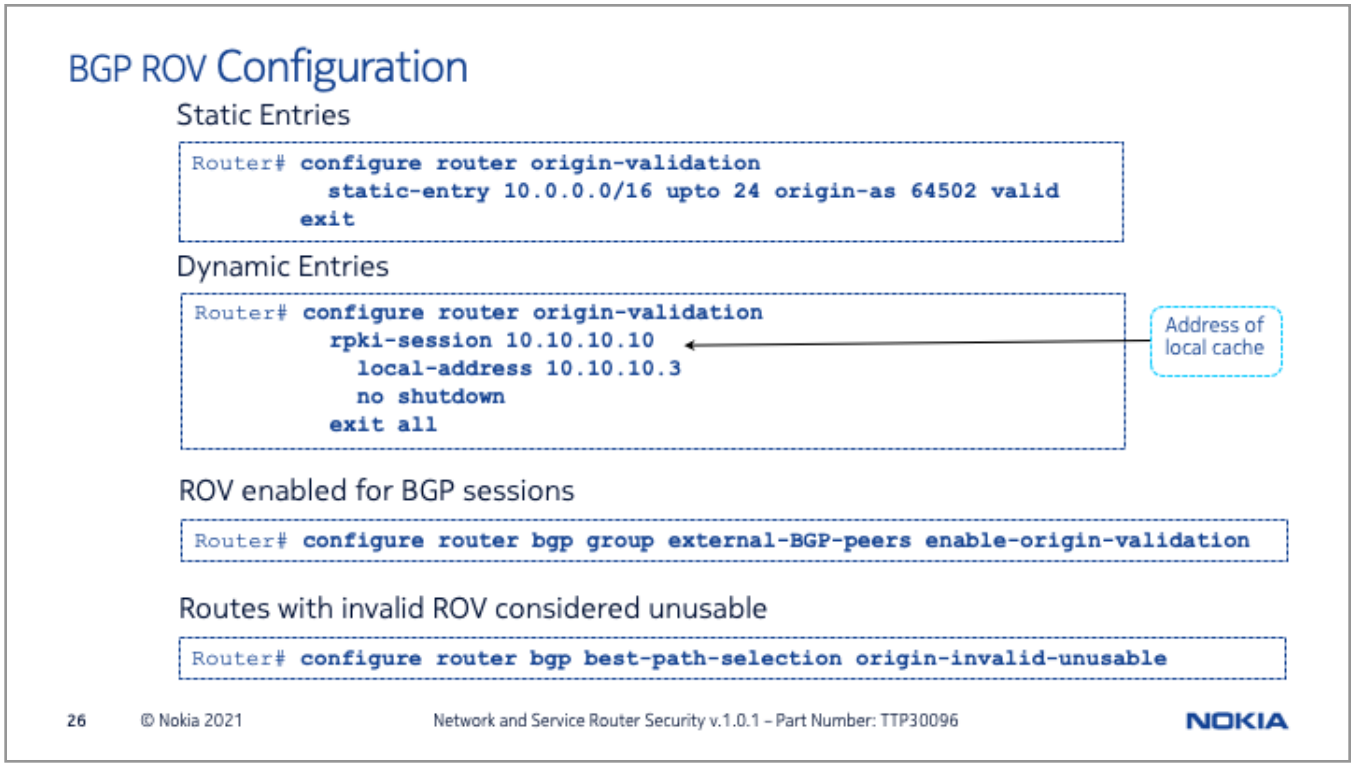
25 © Nokia 2021 Network and Service Router Security v.1.0.1 – Part Number: TTP30096 NOKIA

3. Distributed Repository

A distributed repository consists of a global directory and a local cache:

- The global directory is distributed among the different RIRs. It stores ROAs and certificates, and is typically accessible to all ISPs and anyone connected to the Internet. RIRs act as policy enforcement points to ensure that certificates are issued for their own allocated IP address range. RIRs also ensure that the database records are manipulated only by authorized resources.
- Local cache servers are deployed in the service provider networks. A local cache server obtains a copy of all available certificates from the global directory. It verifies the signature of each certificate and validates each EE certificate by verifying the SIA and AIA records along the certification path. A local cache server retrieves digitally signed ROAs from the global RPKI and then cryptographically validates the ROAs before passing the information to the routers. A local cache periodically refreshes its database to keep it up-to-date.
  A local cache may contain static and dynamic entries. A statically configured entry indicates whether a specific prefix and AS combination is valid. Dynamic entries are learned from the global directory.

A router uses the RPKI-RTR protocol to communicate with the RPKI local cache servers. The RPKI-RTR protocol is a TCP-based transport protocol that is described in RFC 6810, *The Resource Public Key Infrastructure (RPKI) to Router Protocol.*



BGP ROV Configuration

A router can use static and/or dynamic ROA entries:

- Static entries are configured on the router. In the slide, the configured static entry indicates that AS 64502 is authorized to originate routes for prefixes within the range 10.0.0.0/16-24.
- Dynamic entries are obtained from a local cache. In the slide, an RPKI session is configured to the local cache 10.10.10.10 using the local address 10.10.10.3.

A BGP session is configured to use the populated database by issuing the enable-origin-validation command under the BGP group or neighbor context.

By default, the Nokia 7750 SR considers BGP routes with an origin validation state of invalid as valid routes, and the origin validation state is not considered as a factor in the BGP decision process. However, two commands are available under the configure router bgp best-path-selection context to change the default behavior:

- origin-invalid-unusable: when enabled, all routes that have an origin validation state of invalid are considered unusable by the BGP decision process. These routes are not used for forwarding and are not advertised to BGP peers.
- compare-origin-validation-state: when enabled, a new step is inserted in the BGP decision process before the comparison of local preference. The new step checks the origin validation state: a route with a valid state is preferred over a route with invalid or not-found state.

How to Purchase

Attend a Class

See global class schedule and register at the following link - nokia.com/networks/training/src/courses

For any program related questions or private training requests, please contact – learning.services@nokia.com

Self-Paced Learning

To purchase self-paced learning, visit the following link - nokia.com/networks/training/src/self-paced

Register for an exam

To register for an exam, visit the following link - nokia.com/networks/training/src/exams