Cisco live!
July 10-14, 2016 • Las Vegas, NV

Your Time Is Now
Securing BGP

Vinit Jain – CCIE# 22854
Twitter - @vinugenie
BRKRST-3179
Agenda

• Introduction

• Securing BGP Connections
  • MD5 Authentication, IPv6 Link-Local Peering
  • TTL Security, eBGP-Multihop

• Secure Inter-Domain Routing (SIDR)
  • ROA, BGP RPKI

• Preventing BGP DDoS Attacks
  • BGP RTBH Filtering, uRPF

• BGP FlowSpec
Introduction

Housekeeping

• Cell Phones

• Who are you?
  ✓ Service Provider
  ✓ Enterprise

• “Advanced” Class
  ✓ Assume BGP Operational Experience
  ✓ Basic configuration
  ✓ Show commands
  ✓ Understand BGP attributes
Securing BGP

Need for Securing BGP

- BGP - The Internet Protocol
- Any small loophole can cause instability in Internet
- Primary focus for attackers and reverse engineers to find vulnerability
- Prone to Man-In-The-Middle (MITM) attacks, Dos / DDoS attacks
- Common vulnerabilities
  - Session Hijacking
  - Bogus Routing
  - DNS Attacks
Securing BGP

Area of focus

- Authentication
- Integrity
- Availability
- Prefix Origin Validation
- AS Path Verification
Securing BGP Connections
Securing BGP Connections

BGP Session Authentication

- MD5 hash based authentication – defined in RFC 2385
- TCP Option 19 – extension to enhance security using BGP MD5 authentication
- Type 7 passwords in configuration – Easy to break
  - Use service password-encryption
  - IOS, XR and NX-OS now support strong AES encryption
- IOS XR supports HMAC-MD5 and HMAC-SHA1-12 cryptographic algorithms for BGP – Configure as part of key chain authentication
  - Both MD5 authentication and key chain based authentication cannot be configured together.
Securing BGP Connections

BGP Session Authentication – Cryptographic Algorithms on IOS XR

```
RP/0/0/CPU0:R2(config)#key chain BGP_PWD
RP/0/0/CPU0:R2(config-BGP_PWD)#key 1
RP/0/0/CPU0:R2(config-BGP_PWD-1)#cryptographic-algorithm ?
  HMAC-MD5       Configure HMAC-MD5 as cryptographic algorithm
  HMAC-SHA1-12   Configure HMAC-SHA1-12 as cryptographic algorithm
  HMAC-SHA1-20   Configure HMAC-SHA1-20 as cryptographic algorithm
  MD5            Configure MD5 as cryptographic algorithm
  SHA-1          Configure SHA-1-20 as cryptographic algorithm

RP/0/0/CPU0:R2(config-BGP_PWD-1)#cryptographic-algorithm HMAC-SHA1-12
RP/0/0/CPU0:R2(config-BGP_PWD-1)#exit
RP/0/0/CPU0:R2(config-BGP_PWD)#exit
RP/0/0/CPU0:R2(config)#router bgp 100
RP/0/0/CPU0:R2(config-bgp)#neighbor 10.1.102.10
RP/0/0/CPU0:R2(config-bgp-nbr)#keychain BGP_PWD
RP/0/0/CPU0:R2(config-bgp-nbr)#commit
```
Securing BGP Connections

BGP Pass-Through

- ASA / PIX offsets TCP sequence number with a random number for every TCP session
  - Causes MD5 authentication to fail
  - ASA strips off TCP option 19

1. Create Acl to permit BGP traffic
2. Create TCP Map to allow TCP option 19
3. Create class-map to match BGP traffic
4. Disable seq number randomization and Enable TCP option 19 in global policy
Securing BGP Connections

BGP Pass-Through – ASA FW Configuration

access-list OUT extended permit tcp host 10.1.12.1 host 10.1.12.2 eq bgp
access-list OUT extended permit tcp host 10.1.12.2 eq bgp host 10.1.12.2
!
access-list BGP-TRAFFIC extended permit tcp host 10.1.110.2 host 10.1.110.10 eq bgp
access-list BGP-TRAFFIC extended permit tcp host 10.1.110.2 eq bgp host 10.1.110.10
!
tcp-map TCP-OPTION-19
tcp-options range 19 19 allow
!
access-group OUT in interface Outside
!
class-map BGP_TRAFFIC
match access-list BGP-TRAFFIC
!
policy-map global_policy
  class BGP_TRAFFIC
    set connection random-sequence-number disable
    set connection advanced-options TCP-OPTION-19
Securing BGP Connections

IPv6 BGP Peering using Link-Local Address

• Link-Local address – manually assigned or automatically generated with FE80+EUI-64 format

• Usually IPv6 peering - formed over Global IPv6 address

• Using Link-Local address for IPv6 peering prevents:
  • The attacker cannot form BGP peering on link-local address
  • Attacker cannot communicate with the either peer over link-local address

```
neighbor link-local-address%Interface-name remote-as asn
```
Securing BGP Connections

**ebgp-multihop**

- BGP packets for EBGP connections are sent with TTL = 1
- Default TTL value when using `ebgp-multihop` command is 255 (if left empty)
- Attackers can spoof the packets and try to establish BGP peering if correct hop-count is not specified
- For peering between two devices over loopback, use `neighbor disable-connected-check` command instead of `ebgp-multihop 2`
  - The directly connected devices are not two hops away
  - BGP performs connected check which stops it from establishing neighborship over loopback
Securing BGP Connections

BGP TTL Security Hack (BTSH)

Problem:

• Hackers spoof BGP messages to R1 as if they are R2
• R1 must use MD5 to filter out the bogus messages
• MD5 validation must be done on the RP (Route Processor)
Securing BGP Connections

BGP TTL Security Hack (BTSH)

- Provides a lightweight mechanism to defend against most BGP spoof attacks
  - Does **NOT** replace the need for MD5 authentication!

- Sender sets the TTL to 255

- Receiver checks for a TTL of 254 for directly connected neighbors
  - A lower acceptable TTL value must be configured for multihop neighbor

- May use BTSH instead of `ebgp-multihop` if you control both ends of the session

- Packets generated by Hackers will have a TTL that is less than 255
  - Easy to compare the TTL value vs. the 255 threshold and discard spoofed packets
  - Discards can be done at the linecard
  - TTL check is much cheaper than MD5
Securing BGP Connections

Filtering using Firewall / ACL

- Filter for BGP packets from specific peers
- Filtering on firewall is much preferred than routers / switches
  - Large ACL entries consume lot of TCAM resources on routers / switches
  - Firewall designed and optimized to performing filtering tasks

```
permit tcp host 1.1.1.1 eq bgp any  
perm it tcp host 1.1.1.1 any eq bgp

permit tcp host 1.1.1.1 eq bgp 2.2.2.2
permit tcp host 1.1.1.1 2.2.2.2 eq bgp
```
Securing BGP Connections

Protecting BGP Traffic with IPSec

• With IPSec tunneling mechanism, the keys are refreshed from time to time
  • Makes it more secure method than using MD5 based authentication.

• IPSec tunnel is not only having secure reachability but even the routing protocol messages are encrypted

• IPSecn tunnel can be used to protect BGP sessions from integrity violations, replay and DoS attacks through its Authentication Header (AH).

• Encapsulated Security payload (ESP) provides higher level of confidentiality.

• Drawbacks – only covers DoS or MiTM attack
  • Has additional cost of memory and CPU resources for encryption and decryption
Secure Inter-Domain Routing (SIDR)
Secure Inter-Domain Routing

Security Issues with Sourcing of BGP Routes

• Any AS can source/announce incorrect prefixes within BGP
  - Either by mistake (most cases)
  - Or with a malicious intent

• In either case, AS can hijack prefixes owned by other AS
  - Has an impact on end-to-end data forwarding

• BGP prefixes can be hijacked by
  - Sourcing a prefix (with better BGP metrics) that is owned by some other AS
  - Sourcing a more specific for a prefix that is owned by some other AS
Securing Inter-Domain Routing

Prefix Hijacking with smaller AS_PATH (same prefix)

```
192.168.10.0/24
192.168.10.0/24
192.168.10.0/24
192.168.10.0/24
```
Securing Inter-Domain Routing
Prefix Hijacking with more specific Prefix Length
Securing Inter-Domain Routing

BGP Prefix Origin Validation

• Mechanism within BGP to identify incorrectly sourced prefixes and prevent them from being selected as BGP Bestpaths

• Provides Origin AS Validation for BGP prefixes

• Solution for
  - YouTube accident
  - 7007 accident (MAI) that affected SPRINT, UUNET and others
  - Any kind of accidental announcements due to incorrect sourcing of BGP prefixes (99% of mis-announcements fall under this category)

• Does NOT solve BGP path hijacking related issues
  - Origin validation does not provide assurance of BGP aspath received in an update message
Secure Inter-Domain Routing

Large ISP Deployment - RPKI

Global RPKI

Asia Cache

NoAm Cache

Euro Cache

in-PoP Cache

in-PoP Cache

in-PoP Cache

in-PoP Cache

in-PoP Cache

in-PoP Cache

Cust Facing

Cust Facing

Cust Facing

Cust Facing

Cust Facing

Cust Facing
Secure Inter-Domain Routing

BGP Prefix Origin Validation - Implementation

- Router Modifications involves implementation of 3 SIDR drafts
- **Draft1**: RPKI Router protocol defined in the ietf draft-sidr-rpki-rtr-protocol12.txt
- Means of communication between a trusted Cache and BGP routers
- Helps create and maintain within BGP a new address-family specific digested RPKI database in form of {IP prefixes, Origin AS} tuples
- **Draft2**: Origin Validation related BGP protocol modifications defined in the IETF draft-ietf-sidr-pfx-validate-01.txt
- Perform Origin AS validation on ASPATHS of received EBGP prefixes
  - Invalidate prefixes with incorrect origin AS
Secure Inter-Domain Routing

BGP Prefix Origin Validation – Implementation (contd…)

• Draft3: BGP RPKI origin validation state announcement defined in the ietf draft-ietf-sidr-origin-validation-signaling-00.txt

• Announce path validation state within an IBGP network
  - Using new extended community defined in draft-ietf-sidr-origin-validation-signaling-00.txt

• Alternate approach to using path validation state community
  - Implementations could translate path validation state into appropriate IBGP parameters that influence BGP Bestpath processing using route policies
RPKI Database and BGP Design

- Input for the RPKI database for a BGP path:
  - BGP prefix/mask-length (X.X.X.X/N or X::X::X/N)
  - Origin-AS
  - If a BGP prefix/mask-len has no covering ROAs in the RPKI DB, the validity of path is “unknown”
  - If the BGP prefix is covered by one or more ROAs in the RPKI database,
    - If any of the covering ROAs maps to the input origin-AS, the validity of the BGP route is “valid”
    - If none of the covering ROAs map to the input origin-AS, the validity of the BGP route is “invalid”
Secure Inter-Domain Routing

RPKI Operation

• The RPKI-Cache-to-Router connectivity can be many-to-many:
  • One RPKI cache can provide origin-AS validation data to multiple routers and one router can be connected to multiple RPKI caches

• A router connects to RPKI servers/caches/peers to download information in order to build special RPKI database that can be used by BGP to validate origin-ASes for the internet routing table

• Typically, origin-AS validation will be done at ASBRs in an AS for paths received from an outside AS (eBGP paths)
Secure Inter-Domain Routing

RPKI Operation

• The ASBRs simply mark the eBGP paths with an origin-AS validity state:
  • **Valid**: There are database prefix sets in RPKI data that covers prefix and one of them has origin-AS number
  • **Invalid**: There are database prefix sets in RPKI data that covers prefix and none of them has the origin-AS number
  • **Unknown**: There are no matching or covering prefixes in RPKI data
Secure Inter-Domain Routing

RPKI Operation

• The routers do not drop or take any other action on the invalid routes up front
  • It is left up to the operator to choose what to do with the path based on their origin-AS validity state through either RPL or some other configuration CLI

• The reception of eBGP paths and the reception of RPKI data are completely decoupled
  • The router will not ask the RPKI caches as it receives BGP prefixes
  • The origin-AS validation data is mostly driven by the RPKI caches which sends data to the routers at their own pace (initial database dump, followed by incremental updates)

• If RPKI data from RPKI cache in the router covers a prefix when eBGP path is received, BGP will be able to validate that path upon reception, marking the path “valid” or “invalid”

• If RPKI data does not have validation data covering a prefix upon receiving an eBGP path, the BGP will mark the path with an “Unknown”
Secure Inter-Domain Routing

Route Origin Authorization (ROA)

- The RPKI database is a set of ROA objects aggregated from the different RPKI cache that the router connects to
- ROA objects provide a mapping between a BGP prefix block and and AS number authorized to originate that block
- An RPKI cache can send any number of ROAs to the router

| ROA            | 172.25.0.0/16-24 | 12343 |

ROA "prefix-block" covers BGP prefixes 172.25.0.0 with minimum mask-length of 16 and maximum mask-length of 24
- ROA covers 172.25.100.0/24
- ROA does not cover 172.25.100.5/32
AS12343 is authorized to announce prefixes covered by the ROA prefix-block
## Origin-AS Validity Check

<table>
<thead>
<tr>
<th>BGP Prefix / Origin-AS</th>
<th>RPKI Database ROAs</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.1/24 AS 300</td>
<td>10/8-20 AS 100</td>
<td>Does not cover BGP prefix</td>
</tr>
<tr>
<td></td>
<td>10.0/16-24 AS 200</td>
<td>Cover BGP prefix</td>
</tr>
<tr>
<td></td>
<td>10.0/16-32 AS 300</td>
<td>Cover BGP prefix / Origin AS matches</td>
</tr>
<tr>
<td>10.0.1/24 AS 400</td>
<td>10/8-20 AS 100</td>
<td>Does not cover BGP prefix</td>
</tr>
<tr>
<td></td>
<td>10.0/16-24 AS 200</td>
<td>Cover BGP prefix</td>
</tr>
<tr>
<td></td>
<td>10.0/16-32 AS 300</td>
<td>Cover BGP prefix</td>
</tr>
<tr>
<td>20.0.1/24 AS 500</td>
<td>10/8-20 AS 100</td>
<td>Does not cover BGP prefix</td>
</tr>
<tr>
<td></td>
<td>10.0/16-24 AS 200</td>
<td>Does not cover BGP prefix</td>
</tr>
</tbody>
</table>

**Questions:**

1. **Valid**
   - 10.0.1/24 AS 300
2. **Invalid**
   - 10.0.1/24 AS 400
3. **Unknown**
   - 20.0.1/24 AS 500
**Secure Inter-Domain Routing**

**BGP Origin-AS Validation with Updated BGP Prefixes**

<table>
<thead>
<tr>
<th>BGP Prefix / Origin-AS</th>
<th>RPKI Database ROAs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>valid</strong></td>
<td></td>
</tr>
<tr>
<td>10.1.1/24</td>
<td>10/8-24 AS 100</td>
</tr>
<tr>
<td><strong>invalid</strong></td>
<td></td>
</tr>
<tr>
<td>20.0.0/24</td>
<td>20.0/16-24 AS 300</td>
</tr>
<tr>
<td><strong>unknown</strong></td>
<td></td>
</tr>
<tr>
<td>30.1.1/24</td>
<td></td>
</tr>
<tr>
<td><strong>invalid</strong></td>
<td></td>
</tr>
<tr>
<td>10.1.2/24</td>
<td></td>
</tr>
</tbody>
</table>

- When either the BGP table or the RPKI database is modified, the two databases must be kept in sync.
- Incoming eBGP prefixes will be verified against the RPKI database before they are downloaded into BGP table.
Secure Inter-Domain Routing
BGP Origin-AS Validation with RPKI DB Update

<table>
<thead>
<tr>
<th>BGP Prefix / Origin-AS</th>
<th>RPKI Database ROAs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>unknown</strong> 10.1.1/24 AS 100</td>
<td>- 10/8-24 AS 100</td>
</tr>
<tr>
<td><strong>invalid</strong> 20.0.0/24 AS 400</td>
<td>+ 20.0/16-24 AS 300</td>
</tr>
<tr>
<td><strong>valid</strong> 30.1.1/24 AS 200</td>
<td>+ 30.0/8-24 AS 200</td>
</tr>
<tr>
<td><strong>unknown</strong> 10.1.2/24 AS 300</td>
<td></td>
</tr>
</tbody>
</table>

- When a new ROA is added or removed from the database, BGP table have to be back-walked to verify relevant prefixes that are affected by the ROA updates.
- BGP table will be always in sync with RPKI database without having any windows of time where the database are out-of-sync.
Secure Inter-Domain Routing

IBGP Signaling of Origin-AS Validity State

Validate origin-AS
- Lookup RPKI DB to find any data covering the prefix
- Only matching data has origin-AS 300, then it is marked as invalid

1.2.3.0/24 AS_PATH: ... 200

Derive validity state from EXTCOMM attribute

1.2.3.0/24 EXTCOMM: invalid

Derive validity state from EXTCOMM attribute
Secure Inter-Domain Routing

IBGP Signaling of Origin-AS Validity State

• When a BGP route is received from outside AS, ASBRs should check this received path for origin-AS validity

• ASBRs that validates the origin-AS should signal the validity state of the route to its iBGP peers through a non-transitive BGP extended community attribute

• Upon receiving validity state information via extended community, iBGP peers can derive the validity state without having to lookup RPKI database

• If a RR receives an validity state in EXTCOMM attribute from an ASBR, RR should not do any prefix validation and simply forward this attribute towards the other ASBRs inside the AS
Secure Inter-Domain Routing

RPKI Configuration

• RPKI configuration supported on both IOS and IOS XR platforms (not on NX-OS)

• Configuration requires:
  • RPKI server
  • TCP Port number – default port 323
  • Refresh Time (optional)

IOS(config-router)#bgp rpki server tcp 172.16.1.100 port 8282 refresh 600

RP/0/0/CPU0:XR(config-bgp)#rpki server 172.16.1.100
RP/0/0/CPU0:XR(config-bgp-rpki-server)#transport tcp port 8282
RP/0/0/CPU0:XR(config-bgp-rpki-server)#refresh-time 600
Secure Inter-Domain Routing

Show bgp rpki server

IOS# show bgp ipv4 unicast rpki servers

... ...

Neighbor Statistics:

Prefixes 19677
Connection attempts: 1
Connection failures: 0
Errors sent: 0
Errors received: 0

!

Local host: 172.16.1.138, Local port: 54334
Foreign host: 172.16.1.100, Foreign port: 8282

IOS XR - Show bgp rpki server summary
Secure Inter-Domain Routing

Show bgp rpki table

<table>
<thead>
<tr>
<th>Network</th>
<th>Maxlen</th>
<th>Origin-AS</th>
<th>Source</th>
<th>Neighbor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.9.0.0/16</td>
<td>24</td>
<td>4788</td>
<td>0</td>
<td>172.16.1.100/8282</td>
</tr>
<tr>
<td>1.9.21.0/24</td>
<td>24</td>
<td>4788</td>
<td>0</td>
<td>172.16.1.100/8282</td>
</tr>
<tr>
<td>1.9.52.0/24</td>
<td>24</td>
<td>4788</td>
<td>0</td>
<td>172.16.1.100/8282</td>
</tr>
<tr>
<td>1.9.53.0/24</td>
<td>24</td>
<td>4788</td>
<td>0</td>
<td>172.16.1.100/8282</td>
</tr>
<tr>
<td>1.9.112.0/24</td>
<td>24</td>
<td>4788</td>
<td>0</td>
<td>172.16.1.100/8282</td>
</tr>
</tbody>
</table>

**IOS XR - show bgp rpki table ipv4**
Secure Inter-Domain Routing

Show bgp rpki table ipv6

```
RP/0/0/CPU0:R4#show bgp rpki table ipv6

<table>
<thead>
<tr>
<th>Network</th>
<th>Maxlen</th>
<th>Origin-AS</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:648:2800::/48</td>
<td>48</td>
<td>5470</td>
<td>172.16.1.100</td>
</tr>
<tr>
<td>2001:660:3203::/48</td>
<td>48</td>
<td>2094</td>
<td>172.16.1.100</td>
</tr>
<tr>
<td>2001:678:3::/48</td>
<td>48</td>
<td>42</td>
<td>172.16.1.100</td>
</tr>
<tr>
<td>2001:67c:224::/48</td>
<td>48</td>
<td>51164</td>
<td>172.16.1.100</td>
</tr>
<tr>
<td>2001:67c:2e8::/48</td>
<td>48</td>
<td>3333</td>
<td>172.16.1.100</td>
</tr>
</tbody>
</table>
```

...
Secure Inter-Domain Routing

Origin-AS Validation Results

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>I*&gt; 1.9.0.0/24</td>
<td>10.1.15.5</td>
<td>1800</td>
<td>0</td>
<td>200</td>
<td>4789 4790 e</td>
</tr>
<tr>
<td>I*&gt; 1.9.1.0/24</td>
<td>10.1.15.5</td>
<td>1800</td>
<td>0</td>
<td>200</td>
<td>4789 4790 e</td>
</tr>
<tr>
<td>I*&gt; 1.9.2.0/24</td>
<td>10.1.15.5</td>
<td>1800</td>
<td>0</td>
<td>200</td>
<td>4789 4790 e</td>
</tr>
<tr>
<td>V*&gt; 1.9.50.0/24</td>
<td>10.1.15.5</td>
<td>1193</td>
<td>0</td>
<td>200</td>
<td>4790 4788 e</td>
</tr>
<tr>
<td>V*&gt; 1.9.51.0/24</td>
<td>10.1.15.5</td>
<td>1193</td>
<td>0</td>
<td>200</td>
<td>4790 4788 e</td>
</tr>
<tr>
<td>V*&gt; 1.9.52.0/24</td>
<td>10.1.15.5</td>
<td>1193</td>
<td>0</td>
<td>200</td>
<td>4790 4788 e</td>
</tr>
<tr>
<td>N*&gt; 34.1.4.0/24</td>
<td>10.1.15.5</td>
<td>1657</td>
<td>0</td>
<td>200</td>
<td>4789 4790 4791 e</td>
</tr>
<tr>
<td>N*&gt; 34.1.5.0/24</td>
<td>10.1.15.5</td>
<td>1657</td>
<td>0</td>
<td>200</td>
<td>4789 4790 4791 e</td>
</tr>
<tr>
<td>N*&gt; 34.1.6.0/24</td>
<td>10.1.15.5</td>
<td>1657</td>
<td>0</td>
<td>200</td>
<td>4789 4790 4791 e</td>
</tr>
</tbody>
</table>
## Secure Inter-Domain Routing

### Origin-AS Validation Results

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 2.1.0.0/16</td>
<td>10.1.46.6</td>
<td>2309</td>
<td>0</td>
<td>300</td>
<td>3215 e</td>
</tr>
<tr>
<td>*&gt; 2.2.0.0/16</td>
<td>10.1.46.6</td>
<td>2309</td>
<td>0</td>
<td>300</td>
<td>3215 e</td>
</tr>
</tbody>
</table>

RP/0/0/CPU0:R4# `show bgp origin-as validity valid`

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 2.12.0.0/16</td>
<td>10.1.46.6</td>
<td>2747</td>
<td>0</td>
<td>300</td>
<td>e</td>
</tr>
<tr>
<td>*&gt; 2.14.0.0/16</td>
<td>10.1.46.6</td>
<td>2747</td>
<td>0</td>
<td>300</td>
<td>e</td>
</tr>
</tbody>
</table>

RP/0/0/CPU0:R4# `show bgp origin-as validity invalid`

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 2.16.0.0/16</td>
<td>10.1.46.6</td>
<td>2747</td>
<td>0</td>
<td>300</td>
<td>e</td>
</tr>
<tr>
<td>*&gt; 2.17.0.0/16</td>
<td>10.1.46.6</td>
<td>2747</td>
<td>0</td>
<td>300</td>
<td>e</td>
</tr>
</tbody>
</table>

RP/0/0/CPU0:R4# `show bgp origin-as validity not-found`
Secure Inter-Domain Routing

RPKI State Advertisement

- Default behavior – BGP does not advertise RPKI states to IBGP peers
- This CLI at the global/global-AF level enables the iBGP signaling of validity state through an extended-community

**IOS**
R1(config)#router bgp 100
R1(config-router)#address-family ipv4 unicast
R1(config-router-af)#neighbor 192.168.2.2 announce rpki state

**IOS XR**
RP/0/0/CPU0:R4(config)#router bgp 100
RP/0/0/CPU0:R4(config-bgp)#address-family ipv4 unicast
RP/0/0/CPU0:R4(config-bgp-af)#bgp origin-as validation signal ibgp
RP/0/0/CPU0:R4(config-bgp-af)#commit
Secure Inter-Domain Routing

RPKI Best Path Calculation

• Validity states do not affect the best path selection process by default
• Can be modified using a configuration knob.

RP/0/0/CPU0:R4#show bgp rpki summary
...
Origin-AS validation is ENABLED globally
Origin-AS validity WILL NOT affect bestpath selection globally
Origin-AS validity signaling towards iBGP is DISABLED globally

RP/0/0/CPU0:R4(config)#router bgp 100
RP/0/0/CPU0:R4(config-bgp)#bgp bestpath origin-as use validity
RP/0/0/CPU0:R4(config-bgp)#address-family ipv4 unicast
RP/0/0/CPU0:R4(config-bgp-af)#bgp bestpath origin-as use validity
Secure Inter-Domain Routing

Including Invalid Paths in Best Path Calculation

• This CLI at the global/global-AF level allows all “invalid” paths to be considered for BGP best path computation
• If configured at the neighbor/neighbor-AF level (must be an eBGP neighbor), then all “invalid” paths from that specific neighbor/neighbor-AF will be considered as best path candidates
• This knob only takes effect when the “use origin-as validity” knob is enabled.

**IOS**

```
router bgp 100
address-family ipv4 unicast
bgp bestpath prefix-validate allow-invalid
```

**IOS XR**

```
router bgp 100
bgp bestpath origin-as allow invalid
address-family ipv4 unicast
bgp bestpath origin-as allow invalid
neighbor 10.1.46.6
    bestpath origin-as allow invalid
    address-family ipv4 unicast
    bestpath origin-as allow invalid
```
Secure Inter-Domain Routing
Route Manipulation using Validity States - IOS

R1(config)#route-map Match_RPKI permit 10
R1(config-route-map)#match rpki valid
R1(config-route-map)#set local-preference 200
R1(config-route-map)#exit
R1(config)#route-map Match_RPKI permit 20
R1(config-route-map)#match rpki invalid
R1(config-route-map)#set local-preference 50
R1(config-route-map)#exit
R1(config)#route-map Match_RPKI permit 30
R1(config-route-map)#match rpki not-found
R1(config-route-map)#set local-preference 100
R1(config-route-map)#exit
R1(config)#router bgp 100
R1(config-router)#address-family ipv4 unicast
R1(config-router-af)#neighbor 10.1.15.5 route-map Match_RPKI in
Secure Inter-Domain Routing
Route Manipulation using Validity States – IOS XR

```
RP/0/0/CPU0:R4(config)#route-policy Match_RPKI
RP/0/0/CPU0:R4(config-rpl)#if validation-state is valid then
   RP/0/0/CPU0:R4(config-rpl-if)#set local-preference 200
   RP/0/0/CPU0:R4(config-rpl-if)#pass
   RP/0/0/CPU0:R4(config-rpl-if)#exit
RP/0/0/CPU0:R4(config-rpl)#if validation-state is invalid then
   RP/0/0/CPU0:R4(config-rpl-if)#drop
   RP/0/0/CPU0:R4(config-rpl-if)#else
   RP/0/0/CPU0:R4(config-rpl-else)#set local-preference 100
   RP/0/0/CPU0:R4(config-rpl-else)#pass
   RP/0/0/CPU0:R4(config-rpl-else)#exit
RP/0/0/CPU0:R4(config)#router bgp 100
RP/0/0/CPU0:R4(config-bgp)#neighbor 10.1.46.6
   RP/0/0/CPU0:R4(config-bgp-nbr)#address-family ipv4 unicast
   RP/0/0/CPU0:R4(config-bgp-nbr-af)#route-policy Match_RPKI in
```
Remote Triggered Black Hole Filtering (RTBHF)
Remote Triggered Black Hole Filtering

Background

- *Distributed Denial of Service (DDOS)* attacks target network infrastructures or computer services by sending overwhelming number of service requests to the server from many sources.

- A network under DDOS attack can face a major service and financial impact and requires immediate mitigation.

- When a network is under DDOS attack, there are many resources such as bandwidth, CPU, memory can be used up along with the target server’s service degradation.
Remote Triggered Black Hole Filtering

Overview

- BGP Remotely Triggered Black Hole (RTBH) filtering is a security technique to mitigate or overcome DDOS attacks.

- The best approach to prevent such network wide impact is to black hole i.e. drop the undesirable traffic.

- RTBH Solution:
  - Destination Based
  - Source Based

- The destination based protection is for a traffic that is destined towards a server internal to the network. The source based protection is for traffic that is the source of the unwanted traffic.
Remote Triggered Black Hole Filtering

Destination Based RTBH - Configuration

• Can be configured in simple 4 steps
• Step 1 - Create a Static Route Destined to Null0
• Step 2 - Create a Route-map or RPL
• Step 3 – Create a Static route towards the destination server pointing to Null0 interface
• Step 4 - Redistribute the Static Route
Destination Based RTBH - Flow

BGP Sent – 172.19.61.1 Next-Hop = 192.0.2.1

Static Route in Edge Router – 192.0.2.1 = Null0

The static route entered in step 1

What happens when the next-hop in the routing table is Null0?

The BGP update sent out after step 2

172.19.61.1 = 192.0.2.1 = Null0

Next-Hop of 172.19.61.1 is now equal to Null0
Remote Triggered Black Hole Filtering

Source Based RTBH

• Destination based RTBH works on destination IP addresses and only prevents return traffic to an infected host. It is effective for connection-oriented protocols
  • Does not prevent traffic flooding or denial of service type traffic from an infected host

• Unicast Reverse Path Forwarding (uRPF) is a similar technique that works on source IP addresses to drop the traffic by sender at the edge of the network

• uRPF performs a Forwarding Information Base (FIB) lookup for the source IP on the router
  • If FIB has the information for source IP, the packet is forwarded towards the destination
  • If reverse path forwarding (RPF) check will fail, and the router drops the packet

ip verify unicast source reachable-via any
BGP FlowSpec
BGP FLowSpec

DDoS Attacks

- Distributed denial-of-service (DDoS) attacks target network infrastructures or computer services by sending overwhelming number of service requests to the server from many sources.

- Server resources are used up in serving the fake requests resulting in denial or degradation of legitimate service requests to be served

- Addressing DDoS attacks
  - Detection – Detect incoming fake requests
  - Mitigation
    - Diversion – Send traffic to a specialized device that removes the fake packets from the traffic stream while retaining the legitimate packets
    - Return – Send back the clean traffic to the server
Remote Triggered Black Hole Filtering

Major Internet Outages

'Immense' network assault takes down Yahoo

Cyber-attacks batter Web heavyweights

Strikes on eBay, Amazon, CNN.com follow Monday Yahoo! attack

February 9, 2009
Web posted at 9:56 a.m. EST (14:56 GMT)
Remote Triggered Black Hole Filtering

The *Exodus* Requirement

“We need a tool to drop packets based on source IP address that can be pushed out to over 60 routers with in 60 seconds, be longer than a thousand lines, be modified on the fly, and work in all your platforms filtering at line rate.”

Provided by Engineers at Exodus during the Feb 2000 DOS Post Mortem
BGP FlowSpec

Web Server

192.168.1.1

Website

Internet
BGp FlowSpec

DDoS Attack

192.168.1.1

Website

DDoS Traffic

DDoS Traffic

Internet
BGP FlowSpec

Black Hole Community Provided by Provider

192.168.1.1

Website

DDoS Traffic

BGP : 192.168.1.1/32
Com. : 64500:666

DDoS Traffic

Internet
BGP FlowSpec
Black Hole Community Provided by Provider

192.168.1.1
Website

DDoS Traffic

BGP : 192.168.1.1/32
Com. : 64500:666

Discard 192.168.1.1

DDoS Traffic

Internet

Discard 192.168.1.1
BGP FlowSpec

Drawback of RTBH

• Great, I have my website back online!
  □ No more DDoS traffic on my network
  □ But no more traffic at all on my website....

• Well, maybe it was not the solution I was looking for....
BGP FlowSpec

Policy Based Routing

• Identification of DDoS traffic: based around a conditions regarding MATCH statements
  • Source/Destination address
  • Protocol
  • Packet size
  • Etc...

• Actions upon DDoS traffic □ Discard
  • Logging
  • Rate-Limiting
  • Redirection
  • Etc...

• Doesn’t this sound as a great solution?
BGP FlowSpec

Pros n Cons..

• Good solution for
  • Done with hardware acceleration for carrier grade routers
  • Can provide chirurgical precision of match statements and actions to impose

• But...
  • Customer need to call my provider
  • Customer need the provider to accept and run this filter on each of their backbone/edge routers
  • Customer need to call the provider and remove the rule after!

• Reality: It won’t happen...
BGP FlowSpec

FlowSpec as Alternative

• Comparison with the other solutions
  • Makes static PBR a dynamic solution!
  • Allows to propagate PBR rules
  • Existing control plane communication channel is used

• How?
  • By using your existing MP-BGP infrastructure
BGP FlowSpec

Overview

- RFC 5575 - A flow specification is an n-tuple consisting of several matching criteria that can be applied to IP traffic. A given IP packet is said to match the defined flow if it matches all the specified criteria.

- A flowspec is said to be n-tuple because there are multiple match criteria’s that can be defined and all the match criteria should be matched.
  - Traffic will not match the flowspec entry if all the tuples are not matched.

- BGP FlowSpec New NLRI – AFI=1 and SAFI=133
BGP FlowSpec

DDoS Mitigation Steps

• Mitigation of DDOS attacks is performed in two steps:
  • Diversion – Send traffic to a specialized device that removes the fake packets from the traffic stream while retaining the legitimate packets.
    • Define match criteria
    • Define action
  • Return – Send back the clean / legitimate traffic to the server.
BGP FlowSpec

DDoS Mitigation

Security Controller

Sample Netflow

DDOS Analyser

DDOS Scrubber

Enterprise Network
BGP FlowSpec

DDoS Mitigation

Security Controller

DDOS Analyser

Sample Netflow

DDOS Scrubber

Enterprise Network
BGP FlowSpec

DDoS Mitigation

DDOS Analyser

Security Controller

BGP flowspec
Flow: DDOS flow
Action: redirect to DDOS scrubber

DDOS Scrubber

Enterprise Network
# BGP FlowSpec – NLRI based on Match Criteria

<table>
<thead>
<tr>
<th>BGP Flowspec NLRI Type</th>
<th>QoS Match Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type 1</td>
<td>Destination IP / IPv6 address</td>
</tr>
<tr>
<td>Type 2</td>
<td>Source IP / IPv6 address</td>
</tr>
<tr>
<td>Type 4</td>
<td>IP / IPv6 Protocol</td>
</tr>
<tr>
<td>Type 4</td>
<td>Source or destination port</td>
</tr>
<tr>
<td>Type 5</td>
<td>Destination port</td>
</tr>
<tr>
<td>Type 6</td>
<td>Source port</td>
</tr>
<tr>
<td>Type 7</td>
<td>ICMP Type</td>
</tr>
<tr>
<td>Type 8</td>
<td>ICMP Code</td>
</tr>
<tr>
<td>Type 9</td>
<td>TCP flags</td>
</tr>
<tr>
<td>Type 10</td>
<td>Packet length</td>
</tr>
<tr>
<td>Type 11</td>
<td>DCSP</td>
</tr>
<tr>
<td>Type 12</td>
<td>Fragmentation bits</td>
</tr>
</tbody>
</table>
# BGP FlowSpec

## NLRI Type based on Action

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>PBR Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x8006</td>
<td>traffic-rate</td>
<td>Drop</td>
</tr>
<tr>
<td>0x8007</td>
<td>traffic-action</td>
<td>Terminal Action + Sampling</td>
</tr>
<tr>
<td>0x8008</td>
<td>redirect-vrf</td>
<td>Redirect VRF</td>
</tr>
<tr>
<td>0x8009</td>
<td>traffic-marking</td>
<td>Set DSCP</td>
</tr>
<tr>
<td>0x0800</td>
<td>Redirect IP NH</td>
<td>Redirect IPv4 or IPv6 Next-Hop</td>
</tr>
</tbody>
</table>
BGP FlowSpec

Configuration – IOS XR

```plaintext
RP/0/0/CPU0:RR_R3(config)#class-map type traffic match-all FS_RULE
RP/0/0/CPU0:RR_R3(config-cmap)#match source-address ipv4 192.168.1.1/32
RP/0/0/CPU0:RR_R3(config-cmap)#match destination-address ipv4 192.168.5.5/32
RP/0/0/CPU0:RR_R3(config-cmap)#exit
RP/0/0/CPU0:RR_R3(config)#policy-map type pbr FS_POLICY_MAP
RP/0/0/CPU0:RR_R3(config-pmap)#class FS_RULE
RP/0/0/CPU0:RR_R3(config-pmap-c)#drop
RP/0/0/CPU0:RR_R3(config-pmap-c)#exit
RP/0/0/CPU0:RR_R3(config-pmap-c)#class class-default
RP/0/0/CPU0:RR_R3(config-pmap-c)#exit
RP/0/0/CPU0:RR_R3(config-pmap-c)#exit
RP/0/0/CPU0:RR_R3(config)#flowspec
RP/0/0/CPU0:RR_R3(config-flowspec)#local-install interface-all
RP/0/0/CPU0:RR_R3(config-flowspec)#address-family ipv4
RP/0/0/CPU0:RR_R3(config-flowspec-af)#service-policy type pbr FS_POLICY_MAP
RP/0/0/CPU0:RR_R3(config)#commit
```

Install the policies locally on the hardware
BGP FlowSpec

Configuration

- Policies are defined on RR or the controller
- Establish BGP peering with other routers in the network over `address-family flowspec`

```
R2(config)#flowspec
R2(config-flowspec)#local-install interface-all
R2(config-flowspec)#address-family ipv4
```
Show flowspec ipv4 nlri internal

R2#show flowspec ipv4 nlri internal
AFI: IPv4
NLRI (hex) : 0x0120C0A805050220C0A80101
Actions      : Traffic-rate: 0 bps  (bgp.1)
Client Version: 0
Unsupported:  FALSE
RT:
  VRF Name Cfg:  0x00
  RT Cfg:        0x00
  RT Registered: 0x00
  RT Resolved:   0x00
Class handles:
  Handle [0]:   4c9da1
  Class Handle Version:  1
  Sequence:       1024

...  
Statistics                  (packets/bytes)
  Matched    :     8/912
  Dropped    :     8/912
Complete Your Online Session Evaluation

• Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 Amazon gift card.

• Complete your session surveys through the Cisco Live mobile app or from the Session Catalog on CiscoLive.com/us.

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online
Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Lunch & Learn
- Meet the Engineer 1:1 meetings
- Related sessions
Thank you
# Internet of Things (IoT) Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEW! IMINS2</td>
<td>An associate level instructor led training course designed to prepare you for the CCNA Industrial certification</td>
<td>CCNA® Industrial</td>
</tr>
<tr>
<td>Managing Industrial Networks with Cisco Networking Technologies (IMINS)</td>
<td>This curriculum addresses foundational skills needed to manage and administer networked industrial control systems. It provides plant administrators, control system engineers and traditional network engineers with an understanding of the networking technologies needed in today's connected plants and enterprises</td>
<td>Cisco Industrial Networking Specialist</td>
</tr>
<tr>
<td>Control Systems Fundamentals for Industrial Networking (ICINS)</td>
<td>For IT and Network Engineers, covers basic concepts in Industrial Control systems including an introduction to automation industry verticals, automation environment and an overview of industrial control networks</td>
<td></td>
</tr>
</tbody>
</table>

For more details, please visit: [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)

Questions? Visit the Learning@Cisco Booth or contact ask-edu-pm-dcv@cisco.com
# Business Transformation Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>For IT and Network Professionals:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Building Business Specialist Skills</td>
<td>- Builds non-technical skills key to ensure business impact and influence. Topics include: business analysis, finance, technology adoption and effective communications.</td>
<td>Cisco Enterprise IT Business Specialist</td>
</tr>
<tr>
<td></td>
<td>- Bridges IT and business impacts of mature and emerging solutions including cloud plus Internet of Everything</td>
<td></td>
</tr>
<tr>
<td><strong>For Technology Sellers:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applying Cisco Specialized Business Value</td>
<td>Builds skills to discover and address technology needs using a business-focused, consultative sales approach</td>
<td>Cisco Business Value Specialist</td>
</tr>
<tr>
<td>Analysis Skills</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executing Advanced Cisco Business Value</td>
<td>Enables customer transformation through business architecture and solution selling expertise</td>
<td>Cisco Certified Business Value Practitioner</td>
</tr>
<tr>
<td>Analysis and Design Techniques</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performing Cisco Business-Focused</td>
<td>Provides skills and an approach to build a strategic roadmap of IT initiatives, aligned to business priorities</td>
<td>Cisco Transformative Architecture Specialist</td>
</tr>
<tr>
<td>Transformative Architecture Engagements</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For more details, please visit: [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)

Questions? Visit the Learning@Cisco Booth or contact [ask-edu-pm-dcv@cisco.com](mailto:ask-edu-pm-dcv@cisco.com)
# Security Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCIE Security</td>
<td>Expert Level certification in Security, for comprehensive understanding of security architectures, technologies, controls, systems, and risks.</td>
<td>CCIE® Security</td>
</tr>
<tr>
<td>Implementing Cisco Threat Control Solutions (SITCS)</td>
<td>Deploy Cisco’s Next Generation Firewall (NGFW) as well as Web Security, Email Security and Cloud Web Security</td>
<td>CCNP® Security</td>
</tr>
<tr>
<td>Implementing Cisco Secure Access Solutions (SISAS)</td>
<td>Deploy Cisco’s Identity Services Engine and 802.1X secure network access</td>
<td>CCNP® Security</td>
</tr>
<tr>
<td>Implementing Cisco Secure Mobility Solutions (SIMOS)</td>
<td>Protect data traversing a public or shared infrastructure such as the Internet by implementing and maintaining Cisco VPN solutions</td>
<td>CCNP® Security</td>
</tr>
<tr>
<td>Implementing Cisco Network Security (IINS 3.0)</td>
<td>Focuses on the design, implementation, and monitoring of a comprehensive security policy, using Cisco IOS security features</td>
<td>CCNA® Security</td>
</tr>
<tr>
<td>Securing Cisco Networks with Threat Detection and Analysis (SCYBER)</td>
<td>Designed for security analysts who work in a Security Operations Center, the course covers essential areas of security operations competency, including event monitoring, security event/alarm/traffic analysis (detection), and incident response</td>
<td>Cisco Cybersecurity Specialist</td>
</tr>
</tbody>
</table>

For more details, please visit: [www.cisco.com/go/securitytraining](http://www.cisco.com/go/securitytraining) or [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)

Questions? Visit the Learning@Cisco Booth or contact ask-edu-pm-dcv@cisco.com
# R&S Related Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCIE R&amp;S Advanced Workshops (CIERS-1 &amp; CIER-2-2) plus Self Assessments, Workbooks &amp; Labs</td>
<td>Expert level trainings including: instructor led workshops, self assessments, practice labs and CCIE Lab Builder to prepare candidates for the CCIE R&amp;S practical exam.</td>
<td>CCIE® Routing &amp; Switching</td>
</tr>
<tr>
<td>· Implementing Cisco IP Routing v2.0</td>
<td>Professional level instructor led trainings to prepare candidates for the CCNP R&amp;S exams (ROUTE, SWITCH and TSHOOT). Also available in self study eLearning formats with Cisco Learning Labs.</td>
<td>CCNP® Routing &amp; Switching</td>
</tr>
<tr>
<td>· Implementing Cisco IP Switched Networks V2.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Troubleshooting and Maintaining Cisco IP Networks v2.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interconnecting Cisco Networking Devices: Part 2 (or combined)</td>
<td>Configure, implement and troubleshoot local and wide-area IPv4 and IPv6 networks. Also available in self study eLearning format with Cisco Learning Lab.</td>
<td>CCNA® Routing &amp; Switching</td>
</tr>
<tr>
<td>Interconnecting Cisco Networking Devices: Part 1</td>
<td>Installation, configuration, and basic support of a branch network. Also available in self study eLearning format with Cisco Learning Lab.</td>
<td>CCENT® Routing &amp; Switching</td>
</tr>
</tbody>
</table>

For more details, please visit: [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)

Questions? Visit the Learning@Cisco Booth or contact [ask-edu-pm-dcv@cisco.com](mailto:ask-edu-pm-dcv@cisco.com)
## Wireless Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
</table>
| • Designing Cisco Wireless Enterprise Networks  
• Deploying Cisco Wireless Enterprise Networks  
• Troubleshooting Cisco Wireless Enterprise Networks  
• Securing Cisco Wireless Enterprise Networks | Professional level instructor led trainings to prepare candidates to conduct site surveys, implement, configure and support APs and controllers in converged Enterprise networks. Focused on 802.11 and related technologies to design, deploy, troubleshoot as well as secure Wireless infrastructure. Course also provide details around Cisco mobility services Engine, Prime Infrastructure and wireless security. | CCNP® Wireless Version 3.0 (Available March 22nd, 2016) |
| Implementing Cisco Unified Wireless Network Essential | Prepares candidates to design, install, configure, monitor and conduct basic troubleshooting tasks of a Cisco WLAN in Enterprise installations. | CCNA® Wireless (Available Now) |
| Deploying Basic Cisco Wireless LANs (WDBWL) | Understanding of the Cisco Unified Wireless Networking for enterprise deployment scenarios. In this course, you will learn the basics of how to install, configure, operate, and maintain a wireless network, both as an add-on to an existing wireless LAN (WLAN) and as a new Cisco Unified Wireless Networking solution. | 1.2 |
| Deploying Advanced Cisco Wireless LANs (WDAWL) | The WDAWL advanced course is designed with the goal of providing learners with the knowledge and skills to successfully plan, install, configure, troubleshoot, monitor, and maintain advanced Cisco wireless LAN solutions such as QoS, “salt and pepper” mobility, high density deployments, and outdoor mesh deployments in an enterprise customer environment. | 1.2 |
| Deploying Cisco Connected Mobile Experiences (WCMX) | WCMX will prepare professionals to use the Cisco Unified Wireless Network to configure, administer, manage, troubleshoot, and optimize utilization of mobile content while gaining meaningful client analytics. | 2.0 |

For more details, please visit: [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)
Questions? Visit the Learning@Cisco Booth or contact ask-edu-pm-dcv@cisco.com
# Design Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designing Cisco Network Service Architectures (ARCH) Version 3.0</td>
<td>Provides learner with the ability to perform conceptual, intermediate, and detailed design of a network infrastructure that supports desired capacity, performance, availability required for converged Enterprise network services and applications.</td>
<td>CCDP® (Design Professional) (Available Now)</td>
</tr>
<tr>
<td>Designing for Cisco Internetwork Solutions (DESGN) Version 3.0</td>
<td>Instructor led training focused on fundamental design methodologies used to determine requirements for network performance, security, voice, and wireless solutions. Prepares candidates for the CCDA certification exam.</td>
<td>CCDA® (Design Associate) (Available Now)</td>
</tr>
</tbody>
</table>

For more details, please visit: [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)
Questions? Visit the Learning@Cisco Booth or contact [ask-edu-pm-dcv@cisco.com](mailto:ask-edu-pm-dcv@cisco.com)
## Service Provider Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploying Cisco Service Provider Network Routing (SPROUTE) &amp; Advanced (SPADVROUTE)</td>
<td>SPROUTE covers the implementation of routing protocols (OSPF, IS-IS, BGP), route manipulations, and HA routing features; SPADVROUTE covers advanced routing topics in BGP, multicast services including PIM-SM, and IPv6; SPCORE covers network services, including MPLS-LDP, MPLS traffic engineering, QoS mechanisms, and transport technologies; SPEDGE covers network services, including MPLS Layer 3 VPNs, Layer 2 VPNs, and Carrier Ethernet services; all within SP IP NGN environments.</td>
<td>CCNP Service Provider®</td>
</tr>
<tr>
<td>Implementing Cisco Service Provider Next-Generation Core Network Services (SPCORE)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edge Network Services (SPEDGE)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Building Cisco Service Provider Next-Generation Networks, Part 1&amp;2 (SPNGN1), (SPNGN2)</td>
<td>The two courses introduce networking technologies and solutions, including OSI and TCP/IP models, IPv4/v6, switching, routing, transport types, security, network management, and Cisco OS (IOS and IOS XR).</td>
<td>CCNA Service Provider®</td>
</tr>
<tr>
<td>Implementing Cisco Service Provider Mobility UMTS Networks (SPUMTS); Implementing Cisco Service Provider Mobility CDMA Networks (SPCDMA); Implementing Cisco Service Provider Mobility LTE Networks (SPLTE)</td>
<td>The three courses (SPUMTS, SPCDMA, SPLTE) cover knowledge and skills required to understand products, technologies, and architectures that are found in Universal Mobile Telecommunications Systems (UMTS) and Code Division Multiple Access (CDMA) packet core networks, plus their migration to Long-Term Evolution (LTE) Evolved Packet Systems (EPS), including Evolved Packet Core (EPC) and Radio Access Networks (RANs).</td>
<td>Cisco Service Provider Mobility CDMA to LTE Specialist; Cisco Service Provider Mobility UMTS to LTE Specialist</td>
</tr>
<tr>
<td>Implementing and Maintaining Cisco Technologies Using IOS XR (IMTXR)</td>
<td>Service Provider/Enterprise engineers to implement, verification-test, and optimize core/edge technologies in a Cisco IOS XR environment.</td>
<td>Cisco IOS XR Specialist</td>
</tr>
</tbody>
</table>

For more details, please visit: [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)

Questions? Visit the Learning@Cisco Booth or contact ask-edu-pm-dcv@cisco.com
# Collaboration Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCIE Collaboration Advanced Workshop (CIEC)</td>
<td>Gain expert-level skills to integrate, configure, and troubleshoot complex collaboration networks</td>
<td>CCIE® Collaboration</td>
</tr>
<tr>
<td>Implementing Cisco Collaboration Applications (CAPPS)</td>
<td>Understand how to implement the full suite of Cisco collaboration applications including Jabber, Cisco Unified IM and Presence, and Cisco Unity Connection.</td>
<td>CCNP® Collaboration</td>
</tr>
<tr>
<td>Implementing Cisco IP Telephony and Video Part 1 (CIPTV1)</td>
<td>Learn how to implement Cisco Unified Communications Manager, CUBE, and audio and videoconferences in a single-site voice and video network.</td>
<td>CCNP® Collaboration</td>
</tr>
<tr>
<td>Implementing Cisco IP Telephony and Video Part 2 (CIPTV2)</td>
<td>Obtain the skills to implement Cisco Unified Communications Manager in a modern, multisite collaboration environment.</td>
<td>CCNP® Collaboration</td>
</tr>
<tr>
<td>Troubleshooting Cisco IP Telephony and Video (CTCOLLAB)</td>
<td>Troubleshoot complex integrated voice and video infrastructures.</td>
<td></td>
</tr>
<tr>
<td>Implementing Cisco Collaboration Devices (CICD)</td>
<td>Acquire a basic understanding of collaboration technologies like Cisco Call Manager and Cisco Unified Communications Manager.</td>
<td>CCNA® Collaboration</td>
</tr>
<tr>
<td>Implementing Cisco Video Network Devices (CIVND)</td>
<td>Learn how to evaluate requirements for video deployments, and implement Cisco Collaboration endpoints in converged Cisco infrastructures.</td>
<td></td>
</tr>
</tbody>
</table>

For more details, please visit: [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)
Questions? Visit the Learning@Cisco Booth or contact [ask-edu-pm-dcv@cisco.com](mailto:ask-edu-pm-dcv@cisco.com)
## Data Center / Virtualization Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introducing Cisco Data Center Networking (DCICN); Introducing Cisco Data Center Technologies (DCICT)</td>
<td>Learn basic data center technologies and skills to build a data center infrastructure.</td>
<td>CCNA® Data Center</td>
</tr>
<tr>
<td>Implementing Cisco Data Center Unified Fabric (DCUFI); Implementing Cisco Data Center Unified Computing (DCUCI) Designing Cisco Data Center Unified Computing (DCUDC) Designing Cisco Data Center Unified Fabric (DCUFD) Troubleshooting Cisco Data Center Unified Computing (DCUCT) Troubleshooting Cisco Data Center Unified Fabric (DCUFT)</td>
<td>Obtain professional level skills to design, configure, implement, troubleshoot data center network infrastructure.</td>
<td>CCNP® Data Center</td>
</tr>
<tr>
<td>Product Training Portfolio: DCNMM, DCAC9K, DCINX9K, DCMDS, DCUCS, DCNX1K, DCNX5K, DCNX7K</td>
<td>Gain hands-on skills using Cisco solutions to configure, deploy, manage and troubleshoot unified computing, policy-driven and virtualized data center network infrastructure.</td>
<td></td>
</tr>
<tr>
<td>Designing the FlexPod® Solution (FPDESIGN); Implementing and Administering the FlexPod® Solution (FPIMPADM)</td>
<td>Learn how to design, implement and administer FlexPod solutions</td>
<td>Cisco and NetApp Certified FlexPod® Specialist</td>
</tr>
</tbody>
</table>

For more details, please visit: [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)
Questions? Visit the Learning@Cisco Booth or contact ask-edu-pm-dcv@cisco.com
# Network Programmability Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrating Business Applications with Network Programmability (NIPBA);</td>
<td>Learn networking concepts, and how to deploy and troubleshoot programmable</td>
<td>Cisco Business Application Engineer Specialist Certification</td>
</tr>
<tr>
<td>Integrating Business Applications with Network Programmability for Cisco ACI (NPBAACI)</td>
<td>network architectures with these self-paced courses.</td>
<td></td>
</tr>
<tr>
<td>Developing with Cisco Network Programmability (NPDEV);</td>
<td>Learn how to build applications for network environments and effectively</td>
<td>Cisco Network Programmability Developer Specialist</td>
</tr>
<tr>
<td>Developing with Cisco Network Programmability for Cisco ACI (NPDEVACI)</td>
<td>bridge the gap between IT professionals and software developers.</td>
<td>Certification</td>
</tr>
<tr>
<td>Designing with Cisco Network Programmability (NPDES);</td>
<td>Learn how to expand your skill set from traditional IT infrastructure to</td>
<td>Cisco Network Programmability Design Specialist</td>
</tr>
<tr>
<td>Designing with Cisco Network Programmability for Cisco ACI (NPDESACI)</td>
<td>application integration through programmability.</td>
<td>Certification</td>
</tr>
<tr>
<td>Implementing Cisco Network Programmability (NPENG);</td>
<td>Learn how to implement and troubleshoot open IT infrastructure technologies.</td>
<td>Cisco Network Programmability Engineer Specialist</td>
</tr>
<tr>
<td>Implementing Cisco Network Programmability for Cisco ACI (NPENGACI)</td>
<td></td>
<td>Certification</td>
</tr>
</tbody>
</table>

For more details, please visit: [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)

Questions? Visit the Learning@Cisco Booth or contact ask-edu-pm-dcv@cisco.com
## Cloud Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding Cloud Fundamentals (CLDFND)</td>
<td>Learn how to perform foundational tasks related to Cloud computing, and the essentials of Cloud infrastructure</td>
<td>CCNA Cloud</td>
</tr>
<tr>
<td>Introducing Cloud Administration (CLDADM)</td>
<td>Learn the essentials of Cloud administration and operations, including how to provision, manage, monitor, report and remediate.</td>
<td></td>
</tr>
<tr>
<td>Implementing and Troubleshooting the Cisco Cloud Infrastructure (CLDINF)</td>
<td>Learn how to implement and troubleshoot Cisco Cloud infrastructure: compute, network, storage.</td>
<td></td>
</tr>
<tr>
<td>Designing the Cisco Cloud (CLDDES)*</td>
<td>Learn how to design private and hybrid Clouds including infrastructure, automation, security and virtual network services</td>
<td>CCNP Cloud</td>
</tr>
<tr>
<td>Automating the Cisco Enterprise Cloud (CLDAUT)*</td>
<td>Learn how to automate Cloud deployments – provisioning IaaS (private, private with network automation and hybrid) and applications, life cycle management</td>
<td></td>
</tr>
<tr>
<td>Building the Cisco Cloud with Application Centric Infrastructure (CLDACI)*</td>
<td>Learn how to build Cloud infrastructures based on Cisco Application Centric Infrastructure, including design, implementation and automation</td>
<td></td>
</tr>
<tr>
<td>UCS Director Foundation (UCSDF)</td>
<td>Learn how to manage physical and virtual infrastructure using orchestration and automation functions of UCS Director.</td>
<td></td>
</tr>
</tbody>
</table>

* Available Q2CY2016

For more details, please visit: [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)

Questions? Visit the Learning@Cisco Booth or contact ask-edu-pm-dcv@cisco.com