Advanced BGP Routing and IXP Management Training Course

26 - 30 Oct 2026

Cairo

3700 € (Per Person)

Ref: #NO9492_278947

Course Introduction / Overview:

The Border Gateway Protocol (BGP) is the foundational routing protocol of the global internet, responsible for exchanging routing and reachability information among autonomous systems. Its complexity and criticality mean that misconfigurations can have far-reaching consequences, impacting network stability and accessibility for millions of users. This course provides a comprehensive exploration of BGP, from its core principles to advanced traffic engineering and security practices. We will delve into the operational realities of managing internet interconnections, with a special focus on the role of Internet Exchange Points (IXPs) in facilitating efficient and cost-effective traffic exchange. Drawing upon foundational concepts discussed by experts like Iljitsch van Beijnum in his works on BGP, this program moves beyond theoretical knowledge. At BIG BEN Training Center, we have designed a curriculum that emphasizes practical application, preparing participants to design, implement, and troubleshoot robust BGP networks. This training course covers essential topics such as BGP path selection, route filtering, scaling techniques with route reflectors, and modern security mechanisms like RPKI. By mastering both the protocol and the strategic aspects of peering at IXPs, participants will gain the expertise needed to manage and scale modern internet infrastructure effectively and securely.

Target Audience / This training course is suitable for:

- Network Engineers and Architects.
- Internet Service Provider (ISP) Technicians.
- Data Center Operations Staff.
- Network Operations Center (NOC) Personnel.
- System Administrators managing network infrastructure.
- IT professionals involved in network design and implementation.
- Cybersecurity professionals focused on network infrastructure security.
- Telecommunications Engineers.

Target Sectors and Industries:

- Telecommunications and Internet Service Providers.
- Data Center and Colocation Services.
- Cloud Computing Providers.
- Large Enterprise Corporations.
- Financial Services and Banking.
- Media and Content Delivery Networks (CDNs).
- Government, Public Sector, and Defense Agencies.
- Higher Education and Research Networks.

Target Organizations Departments:

- Network Engineering and Design.
- IT Infrastructure and Operations.
- Network Operations Center (NOC).
- Information Security and Cybersecurity.
- Research and Development.
- Technical Support and Escalation Teams.
- Strategic Planning and Technology.

Course Offerings:

By the end of this course, the participants will have able to:

- Master the fundamentals of BGP, including session establishment and path attributes.
- Implement and troubleshoot eBGP and iBGP peering sessions effectively.
- Utilize BGP attributes like Local Preference, MED, and AS Path for traffic engineering.
- Design and apply robust route filtering policies using prefix lists and route maps.
- Configure scalable BGP architectures using route reflectors and confederations.
- Understand the architecture and operational model of an Internet Exchange Point (IXP).
- Develop and analyze peering policies for effective interconnection.
- Secure BGP sessions and routing information using modern best practices like RPKI.
- Troubleshoot common BGP routing problems and network instability issues.
- Leverage tools like Peering DB for managing interconnection relationships.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive, ensuring participants gain both theoretical knowledge and hands-on skills. We believe that complex topics like BGP and IXP management are best learned by doing. Therefore, the course heavily features hands-on lab sessions where participants will configure, manage, and troubleshoot BGP on virtualized network equipment, simulating real-world scenarios. The learning process is enriched with detailed case studies of major internet routing incidents and successful peering strategies. Our expert instructors facilitate group discussions and collaborative problem-solving activities, encouraging participants to share experiences and learn from one another. The curriculum balances formal instruction with interactive workshops, Q&A sessions, and continuous feedback to address individual learning needs. This blended approach ensures that participants not only understand the concepts but can also confidently apply them to their own network environments, translating classroom learning into tangible operational improvements. The focus is on building practical expertise that is immediately applicable in a professional setting.

Course Agenda (Course Units):

Unit One: Fundamentals of BGP and Internet Routing

- Introduction to Autonomous Systems (AS) and BGP's role.
- Understanding Path Vector Protocol mechanics.
- Differences between Internal BGP (iBGP) and External BGP (eBGP).
- BGP message types and neighbor states.
- Basic BGP neighbor configuration and verification.
- Advertising networks into BGP.
- The concept of the BGP routing table (RIB).

Unit Two: BGP Path Attributes and Route Selection

- Detailed exploration of BGP path attributes (PAs).
- Well-known mandatory, well-known discretionary, and optional PAs.
- In-depth analysis of AS_PATH, NEXT_HOP, and ORIGIN.
- Using LOCAL_PREF and MED for traffic influence.
- Understanding the BGP best path selection algorithm.
- Practical labs on manipulating path attributes.
- Introduction to traffic engineering concepts with BGP.

Unit Three: Advanced BGP Policies and Scaling Techniques

- Implementing route filtering with distribute lists and prefix lists.
- Advanced policy control using route maps.
- Understanding and using BGP community strings for policy.
- Challenges of a full-mesh iBGP and solutions.
- Designing and configuring BGP Route Reflectors.
- Implementing BGP Confederations as an alternative scaling method.
- Techniques for route summarization and aggregation.

Unit Four: BGP Security and Troubleshooting

- Common BGP security threats like route hijacking and leaks.
- Implementing BGP neighbor authentication.
- Introduction to Resource Public Key Infrastructure (RPKI) for route origin validation.
- Mutually Agreed Norms for Routing Security (MANRS) initiative.
- Common BGP troubleshooting commands and techniques.
- Analyzing BGP update messages for problem diagnosis.
- Best practices for logging, monitoring, and alerting for BGP.

Unit Five: Internet Exchange Points (IXPs) and Peering Strategy

- The role and architecture of Internet Exchange Points (IXPs).
- Benefits of peering at an IXP versus private interconnects.
- Understanding peering models: bilateral vs. multilateral.
- The function of an IXP route server.
- Developing a strategic peering policy.
- Using Peering DB to find and manage peering relationships.
- Operational and economic considerations of interconnection.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

Considering the increasing centralization of the internet through a few major cloud providers, how might the role and architecture of neutral Internet Exchange Points evolve to ensure a decentralized and resilient global network?

What unique qualities does this course offer compared to other courses?

This training course distinguishes itself by providing a holistic and integrated view of internet routing, uniquely combining deep technical mastery of the BGP protocol with the strategic and operational realities of interconnection at Internet Exchange Points. While many courses focus solely on the command-line configuration of BGP, our curriculum delves into the "why" behind the "how". We explore the business and policy decisions that drive peering strategies, preparing participants not just as technicians but as network architects who understand the economic and performance implications of their routing decisions. The program places a strong emphasis on modern security best practices, dedicating significant time to RPKI and the MANRS framework, which are critical for protecting today's network infrastructure but often overlooked in standard training. Furthermore, the course is built around real-world case studies and hands-on labs that simulate complex interconnection scenarios, moving beyond simple textbook examples. This dual focus on protocol expertise and strategic peering management equips participants with a comprehensive skill set to build, manage, and secure scalable, efficient, and resilient internet-facing networks.