פרוטוקול BGP

מהו פרוטוקול ה- BGP?

Border Gateway Protocol (BGP) הוא מרכיב חיוני בתשתית האינטרנט, המתפקד כפרוטוקול Path Vector בקטגוריה הרחבה יותר של Exterior Gateway Protocols (EGP). תפקידו העיקרי הוא לנהל את אופן ניתוב הנתונים על פני מערכות אוטונומיות שונות (AS) באינטרנט. מערכת אוטונומית היא אוסף של רשתות IP ונתבים שנשלטים על ידי ישות אחת, בדרך כלל ספק שירותי אינטרנט (ISP), ומציגות מדיניות ניתוב מאוחדת לאינטרנט.

בהפעלת BGP, רשתות מייצרות חיבורים ומחליפות מידע ניתוב באמצעות הפעלות של BGP בין נתבים ייעודיים, המכונים "שכנים" או "עמיתים". עמיתים אלה מתקשרים כדי לשתף מידע על הנתיבים הטובים ביותר לניתוב נתונים ליעדים שונים באינטרנט.

תכונה מרכזית של BGP היא היכולת שלה לשמור על טבלאות נרחבות המאחסנות שפע של מידע ניתוב. טבלאות אלו חיוניות לקביעת הנתיבים היעילים ביותר להעברת נתונים. BGP מייחד את עצמו על ידי שימוש בתכונות שונות בטבלאות אלה, המשמשות לאופטימיזציה של החלטות ניתוב. תכונות אלו כוללות פרטים כמו ה-AS-Path, Next-Hop ו-Multi-Exit Discriminator, שכל אחד מהם ממלא תפקיד בהנחיית הבחירה של נתיבי הניתוב הטובים ביותר.

העיצוב של BGP מאפשר לה להתמודד עם מספר עצום של מסלולים, מה שהופך אותה לניתנת להרחבה ומתאימה לתשתית הרשת הנרחבת והצומחת של האינטרנט. בנוסף, הגמישות שלו בניתוב מבוסס מדיניות מאפשרת למפעילי רשתות להגדיר מדיניות ספציפית המשפיעה על תהליך בחירת הנתיב ולנהל את זרימת התעבורה בהתאם לדרישותיהם.

במהותו, BGP הוא חלק בלתי נפרד מהתפקוד של האינטרנט, ומאפשר לרשתות שונות לתקשר ולהחליף נתונים בצורה חלקה. ללא BGP, מבנה הרשת המחובר שמגדיר את האינטרנט לא יוכל לפעול ביעילות, ולהשפיע על זרימת המידע העולמית.

איך פרוטוקול ה-BGP עובד?

BGP פועל באופן מורכב אך מובנה כדי לנהל ניתוב נתונים ברחבי האינטרנט, במיוחד בין מערכות אוטונומיות שונות (AS). כאשר נתב ברשת צריך לשלוח נתונים לרשת אחרת, הוא מסתמך על BGP כדי לקבוע את הנתיב הטוב ביותר. BGP, בניגוד לפרוטוקולי ניתוב מסוימים, אינו משתמש במדדים כמו מרחק או ספירת קפיצות כדי לקבוע את הנתיב הטוב ביותר. במקום זאת, הוא מתמקד במדיניות רשת ובתכונות נתיב.

כל נתב המריץ BGP במערכת אוטונומית מתקשר עם נתבי BGP אחרים, במיוחד אלה שבמערכות אוטונומיות שכנות. תקשורת זו חיונית להחלפת מידע על נתיבים זמינים ליעדי רשת שונים. נתבי BGP יוצרים קשרים, הידועים בשם BGP sessions, עם שכנים אלה. הפרוטוקול מבטיח שלכל הנתבים יש תצוגה עקבית של הטופולוגיה של הרשת.

עבור BGP, בחירת הנתיב הטוב ביותר כרוכה בהערכת כל הנתיבים הזמינים שחבילת רשת יכולה לקחת ולאחר מכן בחירת המסלול על סמך מאפיינים ומדיניות שונים. תהליך קבלת החלטות זה מושפע ממספר

גורמים, כולל אורך נתיב ה-AS, מדיניות רשת שנקבעה על ידי מנהלי מערכת ומאפיינים שונים אחרים כגון local preference, origin type ו- next-hop address.

היבט קריטי בפעולה של BGP הוא השימוש שלו ב-TCP ליצירת קשרים בין עמיתים. BGP משתמש TCP port 179 למטרה זו. הבחירה ב-TCP משמעותית משתי סיבות עיקריות. ראשית, TCP מספקת אספקה אמינה ומסודרת של חילופי מידע ניתוב, מה שמבטיח את שלמות הנתונים. שנית, השימוש ב-TCP מאפשר תקשורת מאובטחת יותר, שכן הוא כולל מנגנון three-way handshake ליצירת חיבור, המסייע באימות נקודות הקצה של הפעלת BGP.

ברגע שנתב BGP קיבל מידע על נתיבים שונים מהשכנים שלו, הוא משתמש באלגוריתם הניתוב שלו כדי לבחור את הנתיב הטוב ביותר. לאחר בחירת הנתיב הטוב ביותר, הנתב מעדכן את טבלת הניתוב שלו ומפיץ מידע זה לעמיתים אחרים ב-BGP, ומבטיח שלכל נתב ברשת יש תצוגה עדכנית של הנתיבים הטובים ביותר לניתוב נתונים.

לסיכום, BGP פועלת על ידי החלפת מידע ניתוב עם נתבים שכנים, הערכת מידע זה על סמך מדיניות רשת ותכונות נתיב, ולאחר מכן שימוש בנתונים אלה כדי לעדכן טבלאות ניתוב ולקבוע את הנתיב הטוב ביותר להעברת נתונים. השימוש של הפרוטוקול ב-TCP מבטיח תקשורת אמינה ומאובטחת בין נתבים.

סוגי ה-BGP

ל-BGP (Border Gateway Protocol) שני סוגים עיקריים: Internal BGP (IBGP) ו- External BGP (EBGP). כל סוג משרת מטרה אחרת בארכיטקטורת הניתוב של האינטרנט.

1. Internal BGP (IBGP):
- מטרה: IBGP משמש להחלפת מידע ניתוב בתוך אותה מערכת אוטונומית (AS). זה חשוב לשמירה על טבלת ניתוב עקבית ומקיפה בתוך ה-AS.
- Administrative Distance (AD): ה-AD הוא ערך המשמש נתבים לבחירת הנתיב הטוב ביותר כאשר ישנם מספר מסלולים לאותו יעד שנלמד באמצעות פרוטוקולי ניתוב שונים. במקרה של IBGP, ערך AD מוגדר בדרך כלל ל-200.
- Time to Live (TTL): ערך ה-TTL ב-IBGP מוגדר בדרך כלל ל-255. ערך TTL גבוה זה משמש כי ייתכן שתקשורת IBGP תצטרך לעבור מספר נתבים בתוך אותו AS, וה-TTL צריך להיות מספיק כדי לאפשר זאת ללא החבילות המושלכות.
2. External BGP (EBGP):
- מטרה: EBGP משמש להחלפת מידע ניתוב בין מערכות אוטונומיות שונות. זה חיוני לאינטרנט בכלל, מכיוון שהוא מאפשר למערכות אוטונומיות שונות לתקשר ולנתב נתונים ביניהם.
- Administrative Distance (AD): ערך ה-AD עבור EBGP מוגדר בדרך כלל ל-20. ערך נמוך יותר זה בהשוואה ל-IBGP אומר שאם נתב לומד על מסלול גם ממקור EBGP וגם ממקור IBGP, הוא יעדיף את מסלול ה-EBGP.
- Time to Live (TTL): ערך ה-TTL עבור EBGP מוגדר בדרך כלל ל-1. הסיבה לכך היא שחיבורי EBGP נוצרים בדרך כלל בין נתבים מחוברים ישירות (AS שכנים). ערך ה-TTL הנמוך עוזר להבטיח שחבילות EBGP לא ינותבו מעבר לשכן המיידי.

1. Adj-RIB-In (Adjacent Routing Information Base-In):
- טבלה זו מאחסנת מידע ניתוב שנלמד מהשכנים. כל נתב BGP מקבל הודעות מסלול מהשכנים שלו, ומסלולים אלו מאוחסנים ב-Adj-RIB-In.
- המידע בטבלה זו כולל את כל המסלולים המפורסמים על ידי שכני BGP, ללא קשר אם מסלולים אלו נבחרו כנתיב הטוב ביותר או לא.
- המסלולים בטבלה זו כפופים למדיניות הייבוא של הנתב, אשר יכולה לשנות או לסנן את המסלולים לפני שהם נחשבים להכללה בטבלת BGP הראשית (Loc-RIB).
2. Adj-RIB-Out (Adjacent Routing Information Base-Out):
- Adj-RIB-Out אחראית לאחסון מידע ניתוב שהנתב מתכוון לפרסם לשכניו.
- לפני שהמסלולים ממוקמים בטבלה זו, הם עוברים עיבוד על סמך מדיניות הייצוא של הנתב. תקנון זה קובע אילו מסלולים מתאימים לפרסום לכל שכן.
- המסלולים ב-Adj-RIB-Out נגזרים בדרך כלל מה-Loc-RIB לאחר החלת מדיניות הייצוא.
3. Loc-RIB (Local Routing Information Base):
- ה-Loc-RIB הוא טבלת הניתוב הראשית של נתב BGP. היא מכילה את המסלולים הטובים ביותר שהנתב בחר בהתבסס על המידע הזמין מ-Adj-RIB-In ומקורות אחרים.
- כל יעד מיוצג על ידי המסלול המועדף ביותר ב-Loc-RIB, המשמש לקבלת החלטות שילוח.
- תהליך בחירת המסלול כולל התחשבות בתכונות BGP שונות, S path length, origin type, next hop, local preference ועוד, כדי לקבוע את הנתיב האופטימלי.

האינטראקציה בין הטבלאות:

- מסלולים מתקבלים מהשכנים ומאוחסנים ב-Adj-RIB-In. מסלולים אלו מעובדים לאחר מכן בהתאם למדיניות הייבוא
- המסלולים הטובים ביותר נבחרים מ-Adj-RIB-In וממוקמים לתוך Loc-RIB.
- לאחר מכן המסלולים ב-Loc-RIB מעובדים בהתאם למדיניות הייצוא וממוקמים ב--Adj-RIB-Out לפרסום לשכנים.

תהליך דינמי זה מבטיח שכל נתב BGP שומר על תצוגה עדכנית של הרשת ומפרסם מסלולים מתאימים לשכניו. בנוסף, כאשר יש שינויים ברשת (כמו הוספת מסלול חדש, ביטול מסלול קיים או תכונות מסלול משתנות), שינויים אלו מתפשטים ברשת באמצעות עדכון הטבלאות הללו. מנגנון זה מאפשר ל-BGP להסתגל באופן דינמי לטופולוגיה המשתנה של האינטרנט, תוך הבטחת ניתוב יעיל ומדויק של נתונים על פני נתיבי רשת מגוונים ומורכבים.

source-update IBGP:

בתצורות BGP, שימוש במשקי loopback להקמת הפעלות BGP משפר את היציבות והאמינות. בניגוד למשקים פיזיים, שיכולים לרדת עקב בעיות חומרה, ממשקי loopback הם וירטואליים ותמיד למעלה כל עוד הנתב פעיל. הגדרה זו מבטיחה שמפגשי BGP יישארו פעילים גם אם קישור פיזי נכשל.

ההבחנה בין IBGP ל-EBGP היא קריטית בתהליך ניתוב BGP. בעוד ש-IBGP עוסק במידע ניתוב בתוך AS, EBGP מטפל בהחלפת מידע ניתוב בין AS שונים. הפרדה זו מסייעת בארגון וניהול נתיבי ניתוב בצורה יעילה ומאובטחת יותר ברחבי הרשת העצומה של האינטרנט.

Connection Collusion:

Connection Collusion ב-BGP היא שיטה אסטרטגית המשמשת כדי לקבוע איזה נתב יזום את חיבור ה-TCP עבור הפעלת BGP, במיוחד כאשר שני הנתבים מוגדרים ליצור חיבור אחד עם השני. גישה זו נועדה למנוע קונפליקטים ולהבטיח התחלה חלקה של מפגש ה-BGP. להלן הסבר מפורט יותר על אופן פעולתו:

1. BGP ו-TCP: BGP מסתמך על TCP, בדרך כלל על יציאה 179, כדי ליצור חיבורים בין נתבים. TCP נבחר בשל מהימנותו ויכולתו להבטיח את שלמות וסדר מידע הניתוב שהוחלף.
2. צורך באסטרטגיית חיבור דטרמיניסטית: בתרחישים שבהם שני נתבים מוגדרים ליצור הפעלת BGP, שניהם יכולים לנסות להפעיל את חיבור ה-TCP בו-זמנית. זה עלול להוביל להתנגשויות חיבור, כאשר הניסיונות של כל נתב להתחבר מפריעים לשני. כדי להימנע מכך, BGP משתמש באסטרטגיה ספציפית כדי להחליט איזה נתב צריך לקחת את ההובלה בהפעלת החיבור.
3. תפקיד מזהה הנתב (Router Id)בקבלת החלטות: ההחלטה איזה נתב יזום את החיבור מבוססת על מזהה הנתב, מזהה ייחודי לכל נתב ב-BGP. מזהה הנתב נקבע בדרך כלל על ידי כתובת ה-IP הגבוהה ביותר בממשקי הנתב, או שהוא יכול להיות מוגדר באופן ידני על ידי מנהל רשת.
4. מזהה נתב גבוה יותר יוזם חיבור: הפרוטוקול מכתיב שהנתב עם מזהה הנתב הגבוה יותר צריך להיות זה שיפעיל את חיבור ה-TCP. המשמעות היא שהנתב עם מזהה הנתב הגבוה יותר שולח תחילה את הודעת SYN (סנכרון), שהוא השלב הראשוני בתהליך לחיצת היד התלת-כיוונית של TCP.
5. היתרונות של Connection Collusion:
- מניעת התנגשויות חיבור: שיטה זו מונעת למעשה את הבעיה של שני הנתבים מנסים להפעיל את החיבור בו-זמנית, מה שעלול להוביל לחיבורים כושלים או מתנגשים.
- הקמת Session יעילה: על ידי קיום כלל ברור ועקבי להפעלת חיבורים, BGP מבטיח הקמה יעילה ומהירה יותר של הפעלות בין נתבים.
- חיזוי ויציבות רשת: האופי הדטרמיניסטי של גישה זו מסייע ליציבות ולחיזוי של הרשת, שהיא חיונית למפעילי רשת ומהנדסים בניהול ופתרון תקלות הרשת.

במהותו, Connection Colllusion ב-BGP הוא מנגנון מוגדר היטב להימנעות מניסיונות חיבור בו-זמניים של שני נתבים. הוא ממנע את מזהה הנתב כדי ליצור תהליך מסודר ונטול קונפליקטים להקמת הפעלות BGP, התורם ליעילות הכללית ולאמינות של פעולות הרשת.

אופן פעולת המנגנון הפנימי של BGP:

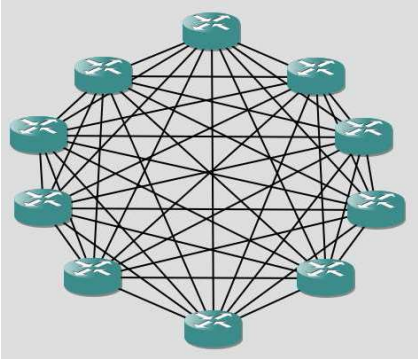
BGP פועל באמצעות מנגנון מתוחכם הכולל ניהול והחלפה של מידע ניתוב בין נתבים. היבט קריטי של אופן פעולת BGP סובב סביב השימוש שלו בטבלאות ניתוב. ישנם בעיקר שלושה סוגים של טבלאות ניתוב ש-BGP מתחזק:

כדי ליישם זאת, הנתב מוגדר לפרסם את כתובת ה-IP של ממשק הלולאה לעמיתים ל-BGP ולהשתמש בכתובת זו כמקור להפעלות BGP. המשמעות היא שמנות BGP נשלחות ומתקבלות בממשק loopback. חשוב גם שכתובת ה-loopback כלולה בפרוטוקולי הניתוב של הרשת, מה שמבטיח שכל העמיתים של BGP יכולים לנתב מנות לכתובת זו.

היתרון של שימוש בממשקי loopback עבור BGP הוא הגמישות המוגברת של הפעלות BGP, שמירה על קישוריות למרות שינויים או שיבושים פיזיים ברשת, מה שמועיל במיוחד ברשתות גדולות ומורכבות.

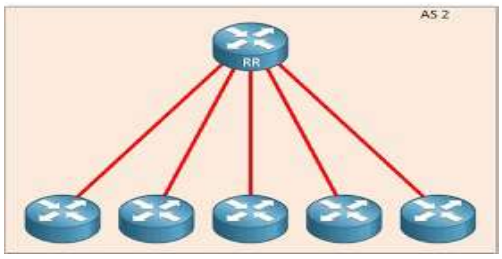
Route Reflectors(RR):

Route Reflectors (RR) ב-BGP מציעים פתרון יעיל לדרישת הרשת המלאה ב-iBGP (Internal BGP). בהגדרת iBGP טיפוסית, כל נתב צריך ליצור סשן הצצה עם כל נתב אחר בתוך אותה AS, מה שמוביל לרשת רשת מלאה (Full mesh). דרישה זו עלולה להפוך לבלתי מעשית ודורשת משאבים ככל שמספר הנתבים ב-AS גדל. מחזירי מסלול עוזרים להפחית בעיה זו.



איך RR עובד:

מחזירי מסלול מרגיעים את דרישת הרשת המלאה בכך שהם מאפשרים לנתבים מסוימים להיות מוגדרים כ-RRs. RRs אלה יכולים לשקף מסלולים שהתקבלו מעמית iBGP אחד לאחר, ובכך להפחית את מספר הפעלות ה-iBGP הנחוצות. נתבים המחוברים ל-Route Reflector מסווגים לשתי קטגוריות:

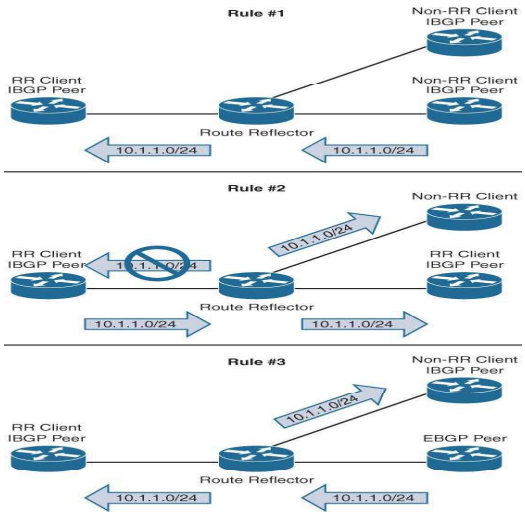


סוגים:

- Route Reflector Clients: אלו הם נתבי iBGP שיש להם קשרי לקוח עם ה-RR. הם צריכים רק ליצור הפעלת BGP עם ה-RR, לא עם כל נתב אחר ב-AS.
- non-client: אלו הם נתבי iBGP שאין להם קשרי לקוח עם ה-RR. הם שומרים על הפעלות ההצצה הסטנדרטיות של iBGP עם נתבים אחרים שאינם לקוח, אך גם מצווים עם ה-RR.

שלושה חוקי RR:

1. Reflection from Non-Clients: כאשר Route Reflector מקבל מסלול מ- non-client,, הוא ישקף מסלול זה ללקוחותיו אך לא ל- non-client. כלל זה מונע לולאות ניתוב ושומר על שלמות פרסומות המסלול.
2. Reflection מלקוחות: אם מתקבל מסלול מלקוחRoute Reflector ישקף אותו לכל לקוחותיו ו-non-client. עם זאת, מכיוון שהלקוחות מקבלים גם עותק של המסלול שהם פרסמו במקור, הם יתעלמו מהמידע הכפול הזה.
3. מסלולים נלמדים של EBGP: מסלולים שנלמדו מעמיתים ל-EBGP מטופלים באופן דומה. ה-RR משקף את המסלולים הללו הן ללקוחות iBGP והן non-client, ומבטיח שכל הנתבים בתוך ה-AS מודעים למסלולים שנלמדו מ-ASes חיצוניים.



סוגי הודעות BGP:

1. OPEN Message:
   - הודעת OPEN היא השלב הראשון בהקמת הפעלת BGP בין שני נתבים.
   - הוא כולל פרטים חיוניים כמו גרסת BGP, מספר AS (מערכת אוטונומית), Hold Time (ברירת המחדל היא 180 שניות), מזהה BGP (בדרך כלל כתובת ה-IP הגבוהה ביותר בנתב), ופרמטרים אופציונליים.
   - גרסת ה-BGP ו-Hold Time חייבים להתאים בין עמיתים כדי שהפעלה תוקם בהצלחה.
2. UPDATE Message:
   - UPDATE Message משמשות להעברת מידע ניתוב.

- הם מורכבים ממסלולים שהוצאו (מסלולים שאינם תקפים עוד), מידע על Network Layer Reachability Information (NLRI) עבור מסלולים חדשים או מעודכנים, ומאפייני נתיב המספקים מידע ניתוב מפורט כמו next-hop ו-preferences, origin הבאה.
- הודעה זו חיונית לעדכון ותחזוקה של טבלאות ניתוב מדויקות בין עמיתים ל-BGP.

3. NOTIFICATION Message:
   - הודעת NOTIFICATION משמשת לדיווח על שגיאות בפעולות BGP.
   - הוא מכיל קוד שגיאה, תת-קוד שגיאה לציון סוג השגיאה ונתונים נוספים המספקים הקשר.
   - קבלת הודעת NOTIFICATION גורמת בדרך כלל לסגירת הפעלת ה-BGP והיא חשובה לפתרון בעיות.
4. KEEPALIVE Message:
   - הודעות KEEPALIVE הן חיוניות לשמירה על הפעלת BGP פעילה.
   - הודעות אלו נשלחות מעת לעת (מרווח ברירת המחדל הוא 60 שניות) ומשמשות כדי למנוע את פסק הזמן של session.
   - הם אינם נושאים תוכן ספציפי; תפקידם העיקרי הוא לאשר את הכדאיות המתמשכת של BGP session.
5. ROUTE REFRESH message:
   - הודעות REFRESH של מסלול משמשות לבקשת עדכון מסלולים מעמית BGP.
   - הודעה זו מאפשרת רענון דינמי של מידע ניתוב ללא צורך בהפעלה מחדש של כל הפעלת BGP.
   - זה שימושי במיוחד בתרחישים שבהם יש צורך במידע מסלול מעודכן מבלי לשבש את חיבור ה-BGP הקיים.

תהליך הקמת השכנות:

ה-BGP (Border Gateway Protocol) Finite State Machine (FSM) הוא תהליך המתאר את השלבים השונים שעוברת session של BGP מהתחלה ועד ליצירת חיבור מלא. הוא מורכב משש מצבים נפרדים BGP session עובר במהלך מחזור החיים שלו. להלן סקירה כללית של כל מדינה:

1. Idle State:
   - במצב Idle, אין חיבור פעיל עם אף עמית BGP.
   - הנתב ממתין להתחיל בתהליך BGP ועדיין לא מנסה ליצור חיבור.
   - בשלב זה, הנתב עשוי לשלוח הודעת SYN להפעלת חיבור TCP ביציאה 179, שהוא השלב הראשון בהקמת הפעלת BGP.
2. Connect State:
   - במצב Connect, הנתב מנסה ליצור חיבור TCP עם עמית BGP.

- במהלך שלב זה, משאבים מוקצים, והודעת OPEN מוכנה להישלח לאחר יצירת חיבור ה-TCP.

3. Active State:

- המצב Active מציין כישלון ביצירת חיבור ה-TCP.
- הנתב ינסה ליצור את החיבור. אם יצליח, הוא יחזור למצב Connect. אם הוא לא מצליח ליצור את החיבור, הוא חוזר למצב Idle.
- במצב זה, הנתב עשוי לנסות לשלוח שוב הודעת OPEN כדי להתחיל מחדש את התהליך.

4. OpenSent State:

- במצב OpenSent, הודעת OPEN נשלחה לעמית, אך הודעת OPEN מתאימה טרם התקבלה בחזרה.
- הנתב ממתין להודעת OPEN מהעמית. לאחר קבלתו, הוא בודק את תקפותו ומצפה להודעה KEEPALIVE. אם מתקבלת הודעה בלתי צפויה, נשלחת הודעת NOTIFICATION לעמית.

5. OpenConfirm State:

- במצב OpenConfirm, הנתב קיבל הודעת OPEN מהעמית וממתין להודעת KEEPALIVE.
- אם הודעת KEEPALIVE לא תתקבל בתוך Hold Time שצוין (בדרך כלל 180 שניות), הנתב יחזור למצב Idle.

6. Established State:

- המצב Established מושג כאשר הודעת KEEPALIVE מתקבלת בהצלחה מעמית ה-BGP.
- בשלב זה, הפעלת BGP מבוססת במלואה, והנתבים יכולים להחליף הודעות UPDATE המכילות מידע ניתוב.
- אם מתרחש כשל או מתקבלת הודעת NOTIFICATION, ההפעלה תחזור למצב קודם, בדרך כלל Idle.

Route Attributs:

Route Attributs ב-BGP משמשות לספק מידע נוסף על מסלולים, המשפיעים על תהליך קבלת ההחלטות לבחירת המסלול. תכונות אלו הן חלק חיוני מהודעות BGP UPDATE. BGP מגדיר מספר סוגים של תכונות מסלול, מסווגות בעיקר לתכונות ידועות ואופציונליות. כל אחת מהקטגוריות הללו מחולקת עוד יותר, כדלקמן:

1. Well-Known Attributes:

- תכונות אלו מזוהות על ידי כל יישומי BGP ויש לטפל בהם כראוי על ידי כל נתבי BGP.
- Mandatory: חייב להופיע בכל הודעת עדכון. כל נתבי BGP צריכים לזהות ולפרש נכון את התכונות הללו.

- Discretionary: מאפיינים אלה עשויים להופיע בהודעת עדכון או לא. הם מזוהים על ידי כל נתבי BGP אך אינם נדרשים בכל הודעה.

2. Optional Attributes:

- תכונות אלו אינן חייבות להיות מוכרות על ידי כל יישומי BGP. הם מספקים מידע מסלול נוסף שעשוי לשמש בנסיבות ספציפיות או למטרות ספציפיות.
- Transitive: אם נתב BGP אינו מזהה תכונה טרנזיטיבית, הוא עדיין יעביר את התכונה לנתבי BGP אחרים. זה מבטיח שהתכונה מופצת ברחבי הרשת, גם אם חלק מהנתבים לא מבינים אותה.
- Non-Transitive: אם נתב BGP אינו מזהה תכונה לא-טרנזיטיבית, הוא לא יעביר את התכונה לנתבי BGP אחרים.

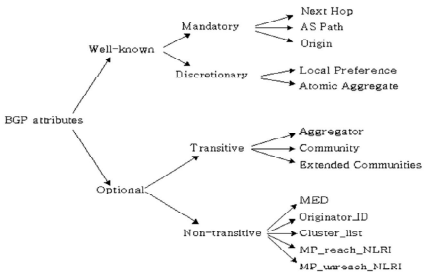
הסבר על Attributes ותהליך בחירת המסלול:

בתהליך בחירת נתיב BGP, תכונות מוערכות באופן שיטתי, על פי היררכיה מוגדרת היטב. זה מבטיח שהנתיב היעיל והאמין ביותר נבחר לניתוב תנועה. הרעף שבו מוערכים תכונות BGP הוא כדלקמן:

1. Weight: תכונה קניינית של Cisco הקובעת את הנתיב המועדף כאשר קיימים מספר מסלולים לאותו יעד. זה משמעותי מכיוון שהוא מאפשר להגדיר העדפה מקומית בנתב אחד מבלי להשפיע על ה-AS כולו. (במקרה זה מתג שאינו תומך בתכונה זו התייחס לתכונה 2 וכ1 , 3 כ-2 וכו'...).
2. Local Preference: משמש להגדרת הנתיב המועדף ליציאה מ-AS, הוא מכתיב את כיוון התנועה בתוך ה-AS. זה משמעותי מכיוון שהוא עוזר לשמור על מדיניות ניתוב פנימית ל-AS וקובע את נקודת היציאה הטובה ביותר מה-AS.
3. Locally Originated: העדפה זו ניתנת למסלולים שמקורם של מהנתב מכיוון שהם בדרך כלל אמינים יותר ודורשים פחות הקפות. הוא משמש כדי להבטיח שימוש יעיל במשאבים פנימיים ולקדם מסלולים בשירות עצמי.
4. AS Path: תכונה זו מפרטת את ה-AS שמסלול עבר כדי להגיע לנתב המקומי. הנתיב עם נתיב ה-AS הקצר ביותר הוא המועדף כי יש להניח שהוא היעיל ביותר ובעל פחות סיכון ללאות.
5. Origin Type: תכונה זו מספקת דרך להעדיף מסלולים שנלמדו מ-IGP על פני אלה מ-EGP או מקורות לא שלמים (כלומר לא ידוע). הוא משמש להעדפת מסלולים פנימיים לאינטרנט וככל הנראה אמינים יותר.
6. MED (Multi-Exit Discriminator): זה מציין את נקודת הכניסה המועדפת ל-AS כאשר זמינות מספר נקודות כניסה. חשוב להשפיע על תנועה נכנסת מ-AS חיצוניים לבחור את נקודת הכניסה האופטימלית ביותר.
7. eBGP על פני iBGP: העדפה זו משמשת מכיוון שמסלולי eBGP נחשבים בדרך כלל לקצרים ומועדפים יותר ממסלולי iBGP, מה שעוזר בבחירת הנתיבים היעילים והאמינים ביותר.
8. IGP Metric: הוא משמש לבחירת הנתיב בעל העלות הנמוכה ביותר כדי להגיע לקפיצה הבאה. מדד זה עוזר בבחירת המסלול שצפוי לקבל את הביצועים הטובים ביותר ב-AS המקומי.
9. הנתיב הישן ביותר: יש להניח כי נתיבים ישנים יותר יציבים יותר, ולכן תכונה זו משמשת להעדפת יציבות בהחלטות ניתוב, תוך הימנעות מהתנופה הפוטנציאלית של נתיבים שיכולה לקרות אם נתיבים חדשים יותר נבחרים כל הזמן.

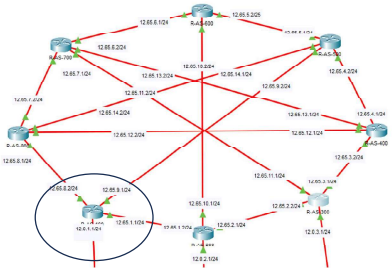
10. Router ID: בהיעדר מבדלים אחרים, תכונה זו משמשת כשובר שוויון. השימוש במזהה הנתב מבטיח שיטה דטרמיניסטית וניתנת לחיזוי לבחירת המסלול.
11. Cluster List Length: זה משמש בתרחישי route reflection כדי למנוע לולאות ניתוב. רשימת אשכולות קצרה יותר מועדפת מכיוון שהיא מציינת פחות route reflection ואפשרות מסלול ישיר יותר.
12. Neighbor Address: שובר השוויון הסופי, הוא משמש לבחירה דטרמיניסטית בין שני נתיבים זהים. בחירת הנתיב עם כתובת ה-IP הנמוכה ביותר מספקת שיטה עקבית ופשוטה לבחירה בין נתיבים כאלה.

תכונות אלו יחד מאפשרות ל-BGP לקבל החלטות ניתוב חכמות הממטבות את בחירת הנתיב לצורך מהימנות, יעילות ועמידה במדיניות הניהולית. הם חיוניים לשמירה על המדרגיות והביצועים של ניתוב בין-דומיינים באינטרנט.



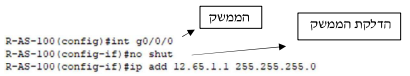
הגדרת טבעת BGP

לפני הכל נגדיר כתובות IP עבור כל ממשק, ראה טפולוגיה:

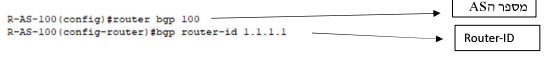


הגדרת כתובות IP לממשקים (ראה טפולוגיה)

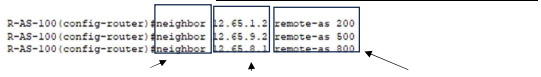
דוגמא מ- R-AS-100



הגדרת Router-Id יחודי בכל נתב (R-AS-100)



הגדרת יחסי שכנות עם הנתבים המחוברים ישירות (R-AS-100)



באיזה AS השכן נמצא	כתובת השכן	שכן

פרסום הרשתות המחוברות ישירות (R-AS-100)

```
R-AS-100(config-router)#network 12.65.8.0 mask 255.255.255.0
R-AS-100(config-router)#network 12.65.9.0 mask 255.255.255.0
R-AS-100(config-router)#network 12.65.1.0 mask 255.255.255.0
R-AS-100(config-router)#network 12.0.1.0 mask 255.255.255.0
```

מסכת הרשת	הרשת המחוברת

הגדרת הפקודה Redistribute static (R-AS-100)

```
R-AS-100(config-router)#redistribute static
```

איזה סוג לחלק	הפקודה עצמה

פקודה זאת רק לנתבים ה-ISP , מהיותם נתבים שהגדרנו ניתוב סטטי.

הוכחה ליחסי שכנות –

```
%BGP-5-ADJCHANGE: neighbor 12.65.1.2 Up
%BGP-5-ADJCHANGE: neighbor 12.65.8.1 Up
%BGP-5-ADJCHANGE: neighbor 12.65.9.2 Up
```

פקודות SHOW-

(R-AS-100) Show ip bgp

```
R-AS-100#show ip bgp
BGP table version is 62, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 12.0.1.0/24      0.0.0.0                  0         0 32768 i
*> 12.0.2.0/24      12.65.1.2                0         0     0 200 i
*                   12.65.9.2                0         0     0 500 400 300 200 i
*                   12.65.8.1                0         0     0 800 700 300 200 i
*> 12.0.3.0/24      12.65.1.2                0         0     0 200 300 i
*                   12.65.9.2                0         0     0 500 400 300 i
*                   12.65.8.1                0         0     0 800 700 300 i
*> 12.1.1.0/24      12.0.1.2                 0         0     0 100 ?
*> 12.1.2.0/24      12.0.1.2                 0         0     0 100 ?
*> 12.2.1.0/24      12.65.1.2                0         0     0 200 ?
*                   12.65.9.2                0         0     0 500 400 300 200 ?
*                   12.65.8.1                0         0     0 800 700 300 200 ?
*> 12.2.2.0/24      12.65.1.2                0         0     0 200 ?
*                   12.65.9.2                0         0     0 500 400 300 200 ?
*                   12.65.8.1                0         0     0 800 700 300 200 ?
```

* הרשת שניתן להגיע , מסמן נתיב אפשרי ו- "-" <" זהו הנתיב הנבחר	הקפיצה הבא כדי להגיע לעיד	ערך תכונה Local weght ו- Prefrence	ה as שהמסלול עובר בהם, AS i של המכשיר ו-i מסמן נלמד על ידי redistribute static

(R-AS-100) Show ip bgp neighbors

```
R-AS-100#show ip bgp neighbors
BGP neighbor is 12.65.1.2,  remote AS 200, external link
  BGP version 4, remote router ID 2.2.2.2
  BGP state = Established, up for 00:14:52
  Last read 00:14:52, last write 00:14:52, hold time is 180, keepalive interval is 60
seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:               46         42
    Keepalives:            15         15
    Route Refresh:          0          0
    Total:                 62         77
  Default minimum time between advertisements runs is 30 seconds
```

AS של השכן ושכן

סוג חיבור EBGP

גרסת BGP ו- Router-ID

מצב השכנות ו-uptime

כל כמה זמן נשלחת הודעת

HoldTime

מידע לשליחה ולקבלה

סוגי הודעות	נשלחו	התקבלו

(R-AS-100) Show ip bgp summary

```
R-AS-100#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 62, main routing table version 6
61 network entries using 8052 bytes of memory
61 path entries using 3172 bytes of memory
55/51 BGP path/bestpath attribute entries using 2752 bytes of memory
8 BGP AS-PATH entries using 192 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 21200 total bytes of memory
BGP activity 23/0 prefixes, 61/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
12.65.1.2       4   200      59      17       62    0    0 00:15:35        4
12.65.9.2       4   500      93      10       62    0    0 00:08:25        4
12.65.8.1       4   800      96       4       62    0    0 00:02:16        4
```

AS

שכנים	גרסת הBGP	באיזה AS	הודעות שהתקבלו	הודעות שנשלחו	גרסת טבלה הBGP	מידע חדש שצריך להישלח או להתקבל	כמות זמן של שכנות

(R-AS-100) Show ip route

```
R-AS-100#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     12.0.0.0/8 is variably subnetted, 27 subnets, 2 masks
C       12.0.1.0/24 is directly connected, GigabitEthernet0/3/0
L       12.0.1.1/32 is directly connected, GigabitEthernet0/3/0
B       12.0.2.0/24 [20/0] via 12.65.1.2, 00:00:00
B       12.0.3.0/24 [20/0] via 12.65.1.2, 00:00:00
```

תמונה זה לא מלאה , אך ניתן לראות שנוספו נתיבים שנלמדו דרך BGP, איזו רשת את ה ad שלהם והקפיצה הבא (ריבועים לפי סדר זה).

NAT

Network address Translation

ברשתות פרטיות, מכשירים משתמשים בכתובות IP פרטיות לתקשורת. כתובות IP אלו מוגדרות כפרטיות מכיוון שהן אינן מוקצות לשום ארגון ספציפי וניתן להשתמש בהן באופן חופשי ללא אישור מיוחד. הטווחים של כתובות IP פרטיות הוקמו כדי להקל על מיצוי כתובות IPv4, מה שמאפשר לארגונים ליישם רשתות פנימיות בקנה מידה גדול מבלי לצרוך שטח (Cider Block) כתובות IP ציבוריות.

מהו NAT :

תרגום כתובות רשת (NAT) הוא פרוטוקול המשמש לשינוי כתובות ה-IP של מקור ו/או יעד של מנות IP כשהן עוברות דרך נתב או חומת אש. המטרה העיקרית של NAT היא לאפשר למחשבים ולהתקנים ברשת פרטית לתקשר עם אחרים באינטרנט הרחב באמצעות כתובת IP ציבורית. זה חיוני, במיוחד מכיוון שכתובות IP פרטיות אינן ייחודיות בעולם ומכאן שאינן ניתנות לניתוב ישירות באינטרנט.

NAT פועל בדרך כלל על גבול הרשת, כגון על נתב או חומת אש. הוא מתרגם את כתובות ה-IP הפרטיות של מכשירים בודדים בתוך רשת מקומית לכתובת IP ציבורית לפני שהנתונים נשלחים לאינטרנט. לעומת זאת, כאשר נתונים מתקבלים מהאינטרנט, NAT מתרגם את כתובת ה-IP הציבורית בחזרה לכתובת ה-IP הפרטית המתאימה של מכשיר היעד בתוך הרשת המקומית.

תהליך זה מאפשר לא רק קישוריות חלקה לאינטרנט עבור התקנים ברשת פרטית אלא גם חוסך בשימוש בכתובות IPv4 שאספקתן מוגבלת ויקרה, שכן התקנים מרובים יכולים לשתף כתובת IP ציבורית אחת. NAT ממלא תפקיד מהותי באינטראקציה של רשתות פרטיות עם האינטרנט, ומגשר על הפער בין הרשת הציבורית העצומה לרשתות פרטיות מקומיות.

איך NAT עובד :

NAT פועל על ידי שינוי כתובות ה-IP של המקור ו/או היעד בכותרות מנות ה-IP. תהליך זה מתרחש כאשר התעבורה עוברת דרך נתב או מכשיר דומה המחבר רשת מקומית לרשת חיצונית, כגון האינטרנט. להלן הסבר פשוט על אופן פעולתו של NAT :

1. Outgoing Traffic (Private to Public Address Translation) :
   - כאשר מכשיר מהרשת המקומית (הפרטית) שולח חבילה לרשת חיצונית, הוא משתמש בכתובת IP פרטית כמקור.
   - כאשר החבילה מגיעה לנתב התומך ב-NAT, הנתב מתרגם את כתובת ה-IP הפרטית הזו לכתובת IP ציבורית. IP ציבורי זה הוא לרוב כתובת ה-IP שהוקצתה לנתב על ידי ספק שירותי האינטרנט (ISP).
   - הנתב שומר על טבלת NAT כדי לעקוב אחר התרגומים הללו, ומשייך את כתובות ה-IP הפרטיות ומספרי היציאה של מנות יוצאות עם כתובת ה-IP הציבורית המתאימה ומספר Port חדש (אם נעשה שימוש בתרגום כתובות יציאה,ראה PAT).
2. Incoming Traffic (Public to Private Address Translation) :
   - עבור מנות נכנסות מהרשת החיצונית, התהליך הפוך.
   - הנתב NAT מקבל את החבילות עם כתובת IP של יעד של הממשק הציבורי שלו.
   - לאחר מכן הוא מתייעץ בטבלת ה-NAT כדי לקבוע את כתובת ה-IP הפרטית ומספר היציאה הנכונים שאליהם יש להעביר את החבילה.
   - הנתב משנה את כתובת ה-IP היעד של החבילה מה-IP הציבורי ל-IP הפרטי המקביל ומעביר אותו למכשיר המתאים ברשת המקומית.

יתרונות NAT :

NAT ממלא תפקיד קריטי ברשתות מודרניות מכמה סיבות :

1. חוסך כתובות IP רשומות כחוק :
   - NAT מאפשר למספר מכשירים ברשת פרטית לשתף כתובת IP ציבורית יחידה הרשומה כחוק. כתובת IP ציבורית זו מסופקת לרוב על ידי ספק שירותי אינטרנט (ISP) והיא ייחודית באינטרנט.
   - באמצעות NAT, לארגונים יכולים להיות רשת שלמה של מכשירים המשתמשים בכתובות IP פרטיות, כולם נגישים לאינטרנט דרך כתובת IP ציבורית אחת. הגדרה זו חיונית בהתחשב בזמינות המוגבלת של כתובות IPv4.
2. מספק פרטיות :
   - NAT משפר את אבטחת הרשת על ידי מיסוך כתובות ה-IP הפנימיות של התקנים ברשת פרטית. כאשר מכשירים מתקשרים דרך האינטרנט, כתובות ה-IP הפרטיות שלהם אינן נחשפות ; רק כתובת ה-IP הציבורית של נתב ה-NAT גלויה.
   - ערפול הכתובות הפנימיות הזה מוסיף שכבה של פרטיות ואבטחה, מה שהופך את זה למאתגר יותר עבור תוקפים פוטנציאליים להתמקד על מכשירים בתוך הרשת הפרטית.