Network Telemetry and Incident Report

Incident ID: MW-2026-008
Status: RESOLVED
Severity: MEDIUM
Report Generated: January 20, 2026 14:30 UTC

Executive Summary

Software configuration error in Midwest Regional Network (Zone MW-5A) caused intermittent routing instability affecting 12,000 subscribers in Minneapolis metro area on January 19, 2026. Issue began following routine BGP policy configuration change intended to optimize traffic routing. Misconfigured route-map caused routing loops and flapping BGP sessions, resulting in 15-45 second service disruptions recurring every 8-12 minutes over 2-hour period. Root cause identified and resolved through configuration rollback. Incident highlights importance of comprehensive pre-change validation and staged deployment procedures for routing changes. No SLA violations; minimal customer impact due to brief, intermittent nature of disruptions.

Incident Timeline

Configuration Change Applied: January 19, 2026, 18:15 UTC
First Routing Anomaly Detected: January 19, 2026, 18:23 UTC (8 minutes post-change)
Pattern Recognition (Routing Loop): January 19, 2026, 18:38 UTC
Escalation to Senior Engineers: January 19, 2026, 18:42 UTC
Root Cause Identified: January 19, 2026, 19:05 UTC (misconfigured route-map)
Configuration Rollback Initiated: January 19, 2026, 19:08 UTC
Service Stabilization: January 19, 2026, 19:15 UTC
Post-Incident Validation: January 19, 2026, 19:15-20:30 UTC
Incident Closed: January 19, 2026, 20:35 UTC
Total Duration: 2 hours 20 minutes (configuration change to incident closure)
Active Instability Period: 52 minutes (18:23-19:15 UTC)

Affected Network Region

Primary Zone: Midwest Regional Network - Zone MW-5A
Geographic Coverage: Minneapolis metro - Downtown Minneapolis, St. Paul, surrounding suburbs
Network Tier: Tier-1 Critical Infrastructure
Subscriber Count: ~98,000 total subscribers in zone
Affected Subscribers: ~12,000 subscribers (12% of zone) experiencing intermittent disruptions
Impact Pattern: Intermittent service disruptions (15-45 seconds) recurring every 8-12 minutes

Services Affected: - Mobile broadband (5G and LTE) - intermittent disruptions - Fixed wireless access - intermittent disruptions - Enterprise connectivity - intermittent packet loss and latency spikes

---

Affected Network Components

Core Routers - Configuration Error

Router: MW-5A-CORE-R01 (Juniper MX960) - **Status:** OPERATIONAL with misconfigured BGP policy (18:15-19:15 UTC) - **Issue:** Route-map configuration error causing routing loops - **Impact:** Flapping BGP sessions, intermittent routing instability - **Resolution:** Configuration rolled back to previous known-good state

Router: MW-5A-CORE-R02 (Juniper MX960) - **Status:** HEALTHY (not directly affected by configuration change) - **Role:** Redundant pair with R01; carried increased traffic load during R01 instability

BGP Sessions - Intermittent Flapping

Affected BGP Sessions (4 of 18 total): - **Peer 1:** Transit Provider A (Zayo) - Flapping every 8-12 minutes - **Peer 2:** Transit Provider B (Level 3) - Flapping every 10-14 minutes - **Peer 3:** Peering Partner (University of Minnesota) - Flapping every 9-13 minutes - **Peer 4:** Internal iBGP session to adjacent zone MW-4C - Flapping every 8-11 minutes

Flapping Pattern: - BGP session established normally - After 8-12 minutes: Route advertisement storm (thousands of route updates sent rapidly) - BGP session hits update limit, enters "idle" state (session down) - After 30-45 seconds: BGP session re-establishes - Cycle repeats every 8-12 minutes

Other BGP Sessions (14 of 18): - Unaffected, remained stable throughout incident

Routing Impact

Routing Loop Formation: Configuration error created scenario where: 1. Router R01 advertises routes to Transit Provider A 2. Transit Provider A advertises routes back to Router R01 (normal) 3. Misconfigured route-map causes R01 to re-advertise these routes AGAIN to Transit Provider A 4. Routes "loop" between R01 and provider, creating infinite routing update cycle 5. BGP update limits triggered, session flaps

Impact on Traffic: - During BGP session down periods (30-45 seconds): Traffic rerouted through R02 or alternate BGP peers - Brief disruption during rerouting (15-20 seconds) - Total disruption per cycle: 15-45 seconds - Frequency: Every 8-12 minutes - Subscribers experienced: Brief connectivity loss or severe latency spike every 8-12 minutes

---

Network Telemetry Summary

Pre-Change Baseline (18:00-18:14 UTC - Normal Operations)

Network Performance: - **Average Latency:** 14ms (intra-zone), 28ms (zone-to-core) - **Packet Loss:** 0.06% (normal) - **Jitter:** 1.6ms (normal) - **Throughput:** 18 Gbps average aggregate traffic - **Connection Success Rate:** 99.92%

BGP Status: - All 18 BGP sessions established and stable - Normal route advertisement/withdrawal rate: 5-10 updates per minute - Routing table: 840,000 routes (full Internet routing table)

Router Performance: - **CPU Utilization:** 38-46% (normal) - **Memory Utilization:** 62% (normal)

Configuration Change Applied (18:15 UTC)

Change Details: - **Objective:** Optimize traffic routing to prefer Transit Provider A for certain destination prefixes (cost optimization) - **Configuration:** Applied route-map to BGP export policy, modifying BGP attributes (local preference, AS path prepending) - **Affected Router:** MW-5A-CORE-R01 only (plan was to apply to R01 first, validate, then apply to R02) - **Change Validation:** Configuration syntax checked (no errors), applied successfully

Incident Window (18:23-19:15 UTC - Routing Instability)

18:23 UTC - First Anomaly: - BGP session to Transit Provider A (Zayo) flapped (went down, came back up) - Monitoring alerts: “BGP Session Down”, “High Route Update Rate” - Initial assessment: Possible provider-side issue

18:32 UTC - Second Flap: - Same BGP session flapped again (9 minutes after first flap) - Route update storm observed: 12,000 route updates in 15 seconds (normal: 5-10/minute) - Pattern emerging: Periodic flapping every ~9 minutes

18:38 UTC - Multiple Sessions Flapping: - 4 BGP sessions now exhibiting flapping behavior - Routing table instability: Routes being added/removed rapidly - Traffic rerouting during flaps causing brief service disruptions - Customer impact beginning: Trouble tickets opened (18 tickets in 15 minutes vs. typical 2-3)

18:42 UTC - Escalation: - Network engineer recognizes pattern as routing loop - Escalated to senior BGP engineers for troubleshooting - Traffic analysis: Identified routing loop involving Transit Provider A

Performance During Instability: - **Latency:** Spikes to 280-450ms during routing transitions (20-32x normal) - **Packet Loss:** Spikes to 8-15% during BGP session down periods (100x+ normal) - **Jitter:** Spikes to 80-120ms during routing transitions (50-75x normal) - **Connection Success Rate:** Drops to 72-85% during disruption cycles - **Customer Experience:** Web pages timing out, video streaming buffering, VoIP calls dropping

Router Performance During Instability: - **CPU Utilization:** Spikes to 88-92% during route update storms (CPU processing BGP updates) - **Memory Utilization:** Increased to 72% (routing table churn consuming memory) - **BGP Update Rate:** 12,000-18,000 updates per event (vs. normal 5-10/minute)

Post-Resolution Performance (19:15-20:30 UTC - Stabilized)

19:15 UTC - Configuration Rollback: - Misconfigured route-map removed from MW-5A-CORE-R01 - Configuration restored to pre-change state - BGP sessions reset and re-established

19:18-19:30 UTC - BGP Reconvergence: - All 18 BGP sessions re-established successfully - Routing table stabilized (840,000 routes) - Route update rate returned to normal (5-10 updates/minute) - No flapping observed for 15+ minutes (pattern broken)

19:30-20:30 UTC - Extended Monitoring: - Network performance returned to baseline - **Average Latency:** 15ms intra-zone, 29ms zone-to-core (normal) - **Packet Loss:** 0.07% (normal) - **Jitter:** 1.8ms (normal) - **Connection Success Rate:** 99.89% (normal) - **BGP Stability:** All sessions stable, no flapping for 1 hour+ (confirms resolution) - **Router CPU:** 42% average (normal)

Detected Issue: BGP Route-Map Misconfiguration Causing Routing Loop

Issue Classification

Primary Issue: Software configuration error - misconfigured BGP route-map creating routing loop
Secondary Issue: Insufficient pre-change validation - configuration error not caught before production deployment
Tertiary Issue: Single-router deployment - change applied to one router without staged validation on non-critical path

Root Cause: Route-Map Configuration Error

Configuration Change Objective: Optimize traffic routing to prefer Transit Provider A (Zayo) for certain destination prefixes to reduce transit costs. Zayo offers better pricing for certain routes (content providers, CDNs, cloud providers).

Implementation Approach: Applied route-map to BGP export policy on MW-5A-CORE-R01, modifying BGP attributes: - Set higher local preference for routes learned from Zayo (prefer these routes for outbound traffic) - Apply AS path prepending for routes advertised to other providers (make routes less attractive, encourage inbound traffic via Zayo)

What Should Have Happened: 1. Learn routes from Zayo 2. Apply higher local preference (prefer Zayo routes for outbound traffic) 3. Advertise our routes to Zayo with normal BGP attributes 4. Advertise our routes to other providers with AS path prepending (make less attractive) 5. **Result:** More traffic flows via Zayo (cost savings)

What Actually Happened (Due to Configuration Error):

Misconfigured Route-Map:

```
route-map OPTIMIZE-ZAYO permit 10
 match ip address prefix-list ZAYO-ROUTES
 set local-preference 150
route-map OPTIMIZE-ZAYO permit 20
 set local-preference 100
 set as-path prepend 65001 65001 65001
```

Configuration Error Explanation: The route-map had two sequence numbers (10 and 20): - Sequence 10: Match routes from Zayo, set local preference 150 (CORRECT - prefer Zayo routes) - Sequence 20: Catch-all (no match statement) applying to ALL OTHER routes, including routes we receive back from providers after advertising to them

The Problem: - We advertise our routes to Zayo (normal) - Zayo advertises these routes back to us (normal BGP behavior - Zayo doesn't know these are our routes after they propagate through Internet) - Route-map sequence 20 (catch-all) matches these routes - Sets local preference 100 and applies AS path prepending - **Then route-map triggers export** - we re-advertise these routes BACK to Zayo - Zayo sees route updates and advertises back to us AGAIN - **Infinite loop:** Routes continuously advertised between us and Zayo

Why BGP Sessions Flapped: BGP has safety mechanisms to prevent routing loops: - **Maximum prefix limit:** Limits number of routes accepted from peer - **Update rate limiting:** Limits rate of route advertisements

When routing loop created thousands of rapid route updates, these safety limits triggered: - BGP session hit update rate limit - Session transitioned to "idle" state (shut down temporarily) - After penalty timer expired (30-45 seconds), session re-established - Loop restarted, cycle repeated

Correct Configuration Should Have Been:

```
route-map OPTIMIZE-ZAYO permit 10
 match ip address prefix-list ZAYO-ROUTES
 set local-preference 150
route-map OPTIMIZE-ZAYO permit 20
 match ip address prefix-list OUR-ROUTES
 set as-path prepend 65001 65001 65001
route-map OPTIMIZE-ZAYO deny 30
 (explicit deny for all other routes - prevents catch-all behavior)
```

Key Difference: Sequence 20 should have explicit match statement (only apply to OUR routes), and sequence 30 should explicitly DENY all other routes (preventing inadvertent re-advertisement of learned routes).

Why Configuration Error Wasn't Caught

Pre-Change Validation Process (What Was Done): 1. ✓ Configuration syntax check

(Juniper configuration parser validated syntax - no errors) 2. ✓ Peer review (junior engineer reviewed configuration - didn’t catch logical error) 3. ✓ Lab testing (tested in lab environment, but test scenario didn’t replicate production conditions)

What Was Missing: 1. ✗ **Comprehensive route filtering validation:** Didn’t verify that only intended routes matched each route-map sequence 2. ✗ **BGP update rate monitoring:** Didn’t monitor BGP update rates during lab testing (loop would have been obvious with monitoring) 3. ✗ **Production-like scale testing:** Lab had only 2-3 BGP peers and small routing table (didn’t replicate production’s 18 peers and 840,000 routes) 4. ✗ **Staged deployment:** Applied change to production router immediately, rather than applying to test router or low-impact path first

Lab Testing Gap: Lab test successfully validated: - Routes from Zayo have higher local preference (correct) - Routes advertised to other providers have AS path prepending (correct)

Lab test FAILED to validate: - Routes received from providers after our advertisements don’t get re-advertised (this is where the bug was) - BGP update rates remain normal (would have detected loop)

Why Lab Test Didn’t Catch Bug: Lab environment had simplified routing table (~5,000 routes vs. production 840,000 routes). The specific scenario that triggered the bug (receiving our own routes back from transit provider after they propagate through Internet) wasn’t present in lab test.

Lesson: Lab testing must replicate production conditions as closely as possible, including scale, number of peers, and representative route behaviors.

Predicted Risk Level: LOW (Post-Resolution, Configuration Corrected)

Risk Score: 2.2 / 10

Risk Assessment Factors: - **Severity:** MEDIUM (during incident) - intermittent disruptions, not complete outage - **Duration:** MODERATE - 52 minutes of active instability - **Customer Impact:** LOW - 12,000 subscribers affected (12% of zone), brief intermittent disruptions - **Business Impact:** MINIMAL - No SLA violations, minimal customer complaints - **Resolution:** SUCCESSFUL - Configuration rolled back, issue resolved - **Recurrence Risk:** VERY LOW - Configuration corrected, process improvements implemented

Business Impact Assessment

Customer Dissatisfaction: - 42 trouble tickets opened during incident (moderate volume) - 120 calls to customer support (manageable) - Customer impact perception: “Network was glitchy for an hour” (annoying but not severe) - Social media: Minimal complaints (brief, intermittent issues less likely to trigger social media complaints than sustained outages)

Revenue Impact: - No SLA violations (consumer services have best-effort SLA, brief intermittent disruptions within tolerance) - No measurable revenue loss - Reputation impact: MINIMAL (incident duration and scope too small for media attention or lasting reputation damage)

Operational Impact: - 2.3 hours of engineering time (incident response, troubleshooting, resolution) - Deferred planned change (traffic optimization) - will need to redesign and retry - Lesson learned: Process improvement needed

---

Root Cause Explanation: Summary

Primary Root Cause:
BGP route-map configuration error creating routing loop due to catch-all route-map sequence inadvertently re-advertising learned routes back to providers.

Contributing Factors: 1. **Configuration Logic Error:** Route-map lacked explicit match statements and deny clause to prevent unintended route matching 2. **Insufficient Pre-Change Validation:** Lab testing didn't replicate production conditions (scale, number of peers, route propagation behaviors) 3. **Lack of Staged Deployment:** Change applied directly to production router without staged validation or gradual rollout 4. **Peer Review Gap:** Reviewer didn't catch logical error in route-map configuration (focused on syntax, not logic)

Human Error: YES - Configuration error was human mistake (engineer misunderstood route-map sequence behavior)

Process Gap: YES - Pre-change validation process didn't catch configuration logic errors; need more comprehensive testing

Preventable: YES - With better testing, staged deployment, or more rigorous peer review, this error would have been caught before production deployment

---

Remediation Actions

Immediate Response (Completed - January 19)

1. Root Cause Identification (19:05 UTC) - Senior BGP engineers analyzed routing table and BGP session behavior - Identified routing loop caused by misconfigured route-map - Confirmed route-map applied at 18:15 UTC correlated with incident start

2. Configuration Rollback (19:08-19:15 UTC) - Removed misconfigured route-map from MW-5A-CORE-R01 - Restored configuration to pre-change state - Reset BGP sessions to force reconvergence with correct configuration

3. Service Stabilization Validation (19:15-20:30 UTC) - Monitored BGP sessions for 1+ hour (no flapping - confirms resolution) - Validated routing table stable and correct - Confirmed network performance returned to baseline - Customer impact ceased (no new trouble tickets after 19:20 UTC)

Short-Term Actions (1-2 Weeks)

4. Configuration Correction and Revalidation (Week of January 22) Priority: MEDIUM
Action: Redesign BGP route-map with explicit match statements and deny clauses to prevent routing loops
Validation: - Comprehensive lab testing with production-scale routing table - BGP update rate monitoring during testing (detect any loops) - Staged deployment: Apply to low-traffic test router first, monitor for 24 hours, then apply to production
Timeline: Complete redesign and testing by January 26; production deployment during next maintenance window (January 31)

5. Enhanced Pre-Change Validation Process (Week of January 22) Priority: HIGH
Action: Implement enhanced change validation requirements for routing changes: - **Mandatory peer review:** Two engineers must review all BGP/routing changes (one junior, one senior) - **Comprehensive test plan:** Test plans must include production-scale scenarios, BGP update rate monitoring, routing loop detection - **Staged deployment:** All routing changes must be deployed to test/low-impact router first, monitored for 24 hours minimum before production deployment - **Rollback plan:** Explicit rollback procedure documented before change approved
Timeline: Process documentation updated by January 24; training for all engineers by January 31

6. BGP Monitoring Enhancement (Week of January 22) Priority: MEDIUM

Action: Deploy enhanced BGP monitoring and alerting: - Real-time BGP update rate monitoring (alert on >100 updates/minute - indicates routing loop or instability) - Automated routing loop detection (identify routes being advertised/withdrawn repeatedly) - BGP session flap detection (alert on repeated session state changes) - Integration with incident management system for automated escalation
Cost: $25,000 (monitoring software + configuration)
Timeline: Deployed by February 5

Medium-Term Actions (1-3 Months)

7. Comprehensive Routing Configuration Audit (February 2026) Priority: MEDIUM
Action: Audit all BGP route-maps, route filters, and routing policies across network: - Identify configurations with catch-all sequences lacking explicit deny clauses - Review for potential routing loop scenarios - Standardize route-map templates with best practices (explicit match statements, deny clauses) - Remediate identified configuration issues
Timeline: 6-8 weeks (audit all zones, remediate issues)
Cost: $60,000 (engineering time + consulting)

8. Network Configuration Validation Automation (Q1-Q2 2026) Priority: STRATEGIC
Action: Implement automated configuration validation tools: - Pre-change validation: Automated syntax and logic checking before configuration applied - Configuration linting: Automated checks for common configuration errors (missing deny clauses, catch-all sequences without matches) - Simulated deployment: Test configurations in emulated network environment before production - Post-change validation: Automated tests confirming expected behavior after change
Cost: $180,000 (software + implementation)
Timeline: Q2 2026 deployment

Best Practices and Lessons Learned

What Worked Well

1. **Rapid Detection:** Monitoring systems detected BGP flapping within 8 minutes of first occurrence
2. **Effective Escalation:** Junior engineer recognized pattern and escalated to senior engineers quickly
3. **Fast Root Cause Identification:** Experienced BGP engineers identified routing loop within 25 minutes
4. **Quick Rollback:** Configuration rollback took only 7 minutes, immediately resolved issue
5. **Minimal Customer Impact:** Brief, intermittent disruptions less severe than sustained outage

What Needs Improvement

1. **Pre-Change Validation:** Lab testing insufficient; didn't replicate production conditions
2. **Peer Review:** Configuration review didn't catch logical error; need more rigorous review process
3. **Staged Deployment:** Change applied directly to production; should use staged deployment
4. **Testing Scale:** Lab environment too simplified; need production-scale test environment

Configuration Best Practices (For BGP Route-Maps)

1. Explicit Match Statements: Every route-map sequence should have explicit match statement defining which routes it applies to. Avoid catch-all sequences without matches.

2. Explicit Deny Clause: Route-maps should end with explicit deny clause (deny all routes not matched by previous sequences). This prevents inadvertent matching of unintended routes.

3. Prefix Lists for Route Filtering: Use prefix lists to explicitly define route sets, rather than relying on implicit matching. This makes configurations more maintainable and less error-prone.

4. Documentation: Comment route-map configurations with intent/purpose of each sequence. This helps future engineers understand logic and avoid errors.

Example - Good Route-Map Configuration:

```
! Purpose: Prefer Zayo transit, prepend AS path to other providers
! Applied to: BGP export policy on MW-5A-CORE-R01
route-map OPTIMIZE-ZAYO permit 10
 description "Prefer routes learned from Zayo"
 match ip address prefix-list ZAYO-ROUTES
 set local-preference 150
route-map OPTIMIZE-ZAYO permit 20
 description "Prepend AS path for our routes to non-Zayo providers"
 match ip address prefix-list OUR-PREFIXES
 set as-path prepend 65001 65001 65001
route-map OPTIMIZE-ZAYO deny 30
 description "Deny all other routes (do not re-advertise learned routes)"
```

Change Management Best Practices

1. Comprehensive Testing: - Lab testing must replicate production scale and conditions - Test plans must include monitoring for side effects (BGP update rates, routing loops, performance impact) - Automated testing where possible

2. Staged Deployment: - Apply changes to test/low-impact systems first - Monitor for 24-48 hours before production deployment - Gradual rollout: One router/zone at a time, validate between stages

3. Rigorous Peer Review: - Two-engineer review for all routing changes (one junior, one senior) - Focus on logic and intent, not just syntax - Reviewer checklist: Common errors to look for

4. Rollback Readiness: - Document rollback procedure before change - Test rollback in lab - Monitor closely post-change with finger on “rollback button”

Technical Metadata

Report Classification: Internal Operations - Incident Review
Data Sources: Router telemetry, BGP session monitoring, network performance monitoring, customer trouble tickets
Analysis Period: January 19, 2026, 18:00-21:00 UTC
Contributors: Network Engineering team (BGP engineers), Network Operations Center, Change Management
Review Status: Reviewed by Senior Network Engineer and Director of Network Engineering
Distribution: Network Engineering teams, NOC staff, Change Management team

Related Incidents: None recent (first routing configuration incident in Zone MW-5A)
Follow-Up Actions: 5 action items assigned (configuration correction, process improvements, monitoring enhancements)
Next Review Date: February 5, 2026 (post-process improvement validation)

End of Report

For questions or additional analysis, contact:
Network Engineering: neteng@pacificwireless.net

Change Management: change-mgmt@pacificwireless.net
Report Author: emily.chen@pacificwireless.net