Cisco Trusted Intelligent Peering

Paul Cernick – Solution Architect
Tony Le – Architecture Product Management
Phil Bedard – Technical Marketing Engineering

May, 2019
Agenda

• Peering Trends & Challenges
• Cisco Secured Intelligent Peering
• Peering Technical Solution
While video dominates...

...other trends are driving advancements in peering design

- Increasing use of SaaS (AWS, Office365, SFDC, etc.) creates stricter SLAs on peering performance
- 5G requirements accelerate relocation of network functions and data storage to distributed locations
Security is top of mind
Your network is under attack, and peering is the gateway

Route Hijacking in 2017
13,935 route leaks and hijacking incidents
38% were considered attacks

Source: Arbor 2018 Worldwide Infrastructure Security Report

Move towards distributed peering

- Content Delivery Networks (CDN) account for 52% of traffic today, 71% by 2021
- As 5G and Mobile Edge Compute evolve, peering and CDN will be driven even closer to the end users

Traditional single peering location in LA transforms into 3 metro peering locations, reducing cost and improving SLAs
How has Peering changed?
“Flattening” of the Internet powered by 2 major transitions

Traditional Content Peering

- Content Provider
- Internet
- SP
- CDN

Optimized Content Peering

- Content Provider
- Internet
- SP
- CDN

- Video will be 82% of Internet traffic by 2021
- Subscriber bandwidth consumption growing at a 31% CAGR
- Direct interconnection, less reliance on transit backup

© 2018 Cisco and/or its affiliates. All rights reserved.
Interconnect eXchange Point growth
From then to now – why it matters

• Allows more users to connect to more content in more places
• IXP offer shared locations where SPs, Content providers, Enterprises can meet and connect
• Growth from ~20 IXP locations to more than 700 worldwide today
• Facilitated the “flattening” of the Internet
Trend towards a more fabric focused design

- Classical Peering

- Horizontal scaling adds resiliency
- Less reliance on long-haul backup for metro or DC Peering
- Reduced blast radius during maintenance or failure
- Simplified SR control-plane

- Greater resiliency and capacity scale
- Optimized feature sets at each layer
- Optimized fabric for both ingress and egress content delivery
- Lower power consumption and rack space usage
Trend towards network function separation

Combined Peering, Core and PE Services

Discrete network elements for each function
Cisco Secured Intelligent Peering Solution

Trusted and secure portfolio
- Trusted platforms with SW run time protection
- Cloud powered BGP security monitoring
- DDoS protection

Intelligent
- Optimization tools helps enhance services
- Simplified design with traffic engineering

Cost optimized
- Distributed peering reduces transport costs
- Flexible Consumption Model with pooling of capacity
- License portability provides investment protection

Power / space optimized
- Highest density in optimized form factor
- 20% lower power compared to leading competition
- Lower Total Cost of Ownership (TCO)

Software driven
- IOS-XR with enhanced BGP protocol stack
- Automation focused
- Open API driven / Programmability
- SDN driven Framework

© 2018 Cisco and/or its affiliates. All rights reserved.
Cisco Peering Platform Options

Cisco Crosswork Automation Suite

EPNM - Provisioning  WAE - WAN Optimization  NSO - Orchestration  Crosswork Network Insights  BGP Monitoring

Services Leadership

ASR 9000

• Industry leading services
• Up to 3.2T/slot line card
• Fixed and modular systems
• IOS-XR, ISSU & high availability
• Trusted HW & MACsec
• DDoS solution

Low Power & Density Leadership

NCS 5500

• Density and low power leadership
• Up to 9.6T/slot line card
• Fixed and modular systems
• IOS-XR & high availability
• Trusted HW & MACsec
• DDoS Solution

© 2018 Cisco and/or its affiliates. All rights reserved.
Trusted Critical Infrastructure
Requires Trusted Service Provider Networks

- Trust Begins in Hardware
  Anti-counterfeit and Trust Anchor Infrastructure

- Verifying Trust: Network OS
  Image Signing and Secure Boot Infrastructure

- Maintaining Trust at Runtime
  Run-time Defense, Encrypted Transport, DDoS Protection

- Visualize and Report on Trust
  Integrity Measurement and Verification Infrastructure

© 2018 Cisco and/or its affiliates. All rights reserved.
Automation portfolio

Implement intent using model-based configuration

NSO
Network Services Orchestrator

Optimize Multi-layer Network

WAE
WAN Automation Engine (+SR-PCE)

Manage a Multi-layer, Multi-service environment

EPNM
Evolved Programmable Network Manager

Open to ecosystem partner:

© 2018 Cisco and/or its affiliates. All rights reserved.
Flexible Consumption Model

- Reduce upfront capital up to 36%
- Utilize capital efficiently
- Protect your investment
- Embedded automation

Customer benefits

- Pay for use
- Portability

Resource pooling
- Embedded automation

Network ports

Year
- Gen #1 line card
- Gen #2 line card

West
- North
- East

© 2018 Cisco and/or its affiliates. All rights reserved.
Cisco Peering architecture design considerations

Traditional Peering

- Widely deployed model in heavy use today
- Common model for SPs, Enterprises, Education, etc.
- Peering role often added organically as network grew
- High density routers with max vertical scale
- Often deployed with integrated vertical network functions
  - Combined Peering, Services PE, and Core
  - Can be migrated to discrete network functions
Cisco Peering architecture design considerations
Migration towards fabric based peering

- Horizontal scaling adds resiliency and capacity
- Reduced blast radius during maintenance or failure
- Lower-cost/price-per-bit
- Increased port count and BW without increasing the cost
- Easier to upgrade
- Less reliance on long-haul backup for metro or DC Peering
- Can be migrated to full fabric design
Cisco Peering architecture design considerations

Fabric based Peering

- Greater resiliency and capacity scale
- Discrete network functions allows optimized feature sets at each layer
- Optimized fabric for both ingress and egress content delivery
- Lower-cost/price-per-bit
- Increased port count and BW without increasing the cost
- Evolution in peering similar to widespread use of ToR devices in data centers
- Operational efficiencies for peering management
- Easier node upgrades, adds, deletes, maintenance
Localized Peering deployment
Optimized content delivery

- Content sources like Netflix placed as close to the user as possible.
- Traditional wireline and wireless service providers have heavy inbound traffic from content providers delivering OTT video.
- Peering nodes connect directly to the metro core enable delivery across the region or metro.
- Drives greater network efficiency
## Cisco Intelligent Peering

### Segment Routing

**Foundation for Network Operations Simplification and Automation, and Service Agility via Programmability**

<table>
<thead>
<tr>
<th>Simplification of network protocols</th>
<th>Automated 50ms convergence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simplification of Traffic Engineering</td>
<td>Built-in Resiliency &amp; HA</td>
</tr>
<tr>
<td>Application enabled policy using SDN techniques</td>
<td>Programmable</td>
</tr>
</tbody>
</table>

**Universal Forwarding Plane**

From Access to Peering
Optimization and SLAs drive Peering SDN

Egress
Best network exit path that is both cost-efficient and provides good user experience metrics (latency, link utilization & traffic loss)

Optimal exit link chosen:
- Low cost (private peer)
- Low utilization link

Ingress
Optimal path across SP network for ingress traffic from peering location to SP end users

Optimal exit link chosen:
- Latency
- Cost
Optimization from peer to network location

Requirements:
- Deliver optimal path for ingress traffic from Peering site to SP end users
- Network optimization to reduce hot spots. Improve performance and allow for capex deferral
- Optimization based on latency and bandwidth constraints

Solution:
- Cisco WAE – Optimization
- SR-PCE – PCEP-SR
- Segment Routing TE – Transport
Optimization from network location to peer

Requirements:
- Drive best exit path that is cost-efficient w/ good user experience metrics (latency, link utilization & traffic loss)

Solution:
- Segment Routing Egress Peer Engineering (EPE)
BGP Hijack Occurrences

There were 13,935 route leaks and hijacking incidents in 2017. 38% were considered attacks.

Nationwide Comcast Outage: Nov. 6, 2017
“The culprit was a configuration issue from Level 3, a telecommunications and internet service provider owned by CenturyLink. In a statement to CNN Tech, CenturyLink said a "configuration error" disrupted service and technicians restored service in 90 minutes.”*

Amazon Route 53 Outage: April. 24, 2018
Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency
Almost 1,300 addresses for Amazon Route 53 rerouted for two hours.

*Source: CNN
Cloud based Network insights monitors at 1000s of points world wide
CCNI Use Case – Route Hijack

- Route Hijacks can be performed in many ways
- Some are malicious, some are accidental.

- Alarm Conditions test for any of the following conditions:
  - ASN Origin Violation
  - Unexpected Longer Prefix Match
  - ROA/RPKI Failure/Miss-match
  - AS Path Length Violation
  - Man in the Middle Detection
Route Leaks can be performed in many ways. Some are accidental, some are complex logical issues.

Layered BGP Policy Alarm Architecture lets you customize monitoring criteria to match your peering architecture intent.

Our Alarm Conditions test for any of the following conditions that can be symptoms of a Route Leak:

- Upstream AS Change (whitelist / blacklist)
- ASN Origin Violation
- Prefix Aggregate Change
- Unexpected Longer Prefix Match
- AS Path Length Violation (too short / too long)
- Peer Router Prefix Violation (whitelist / blacklist)

Provider B allows Customer to peer A.B.C.D/28 as a non-portable block. Customer accidentally advertises A.B.C.D/24 from Provider B towards Provider A.
DDoS Attacks are increasing and more sophisticated

- SPs are seeing an ever increasing number of DDoS Attacks
- 61% of Netscout Arbor Infrastructure survey respondents saw > 10 attacks per month
- 22% experiences more than 500 DDoS attacks per month

- Attacks are not simple volumetric attacks anymor
- Multi-vector attacks are increasing using volume and application layer attacks together
Distributed Denial of Service (DDoS) for Peering Solutions

- Real Time Telemetry with Netflow
- Automated mitigation using high-scale ACL and BGP Flowspec

DDoS Solution Partners

© 2018 Cisco and/or its affiliates. All rights reserved.
Cisco Intelligent Peering - Extracting Data

Advanced automation, analytics, and visibility requires network data

Granular periodic and event driven data @ much higher scale and speed vs SNMP
Use Telemetry Data to Its Full Potential: Crosswork Health Insights

**Smart Monitoring**
- Recommendation Engine
  - Automatically determine Network KPIs of relevance and start monitoring them

**Smart Filtering**
- Anomaly Detection
  - Network KPI Baselining and Dynamic Thresholds. Deviation Alert.
  - Establish baseline with short and long-term seasonality built-in

**Smart Remediation**
- Signature Matching
  - Alert and automatically deploy fixes if network conditions match prior observed anomalies
Automating Peering Changes
Crosswork Change Automation

Framework

- Network Automation Alerting Service
- Real-time tracking of network state
- Multi-protocol Data Collection Service

Change Automation

- Continuously Checks Engine
- APIs
- Multi-layer Configuration Deployment Service

Functionality

- Built around Ansible
- User defined: Network change workflow expressed as an Ansible Playbook (Ansible YAML syntax)
- Each workflow step is a “play”
- Read plays (check CPU usage, ...), Write plays (configure interface, protocol, s/w upgrade, ...)
- Closed Loop
- Concurrent monitoring - continuous real-time tracking of network state by read plays
- Write plays verify network state against intended state
- Scale-out, single stepping, break pointing
- Direct (shell) and Web UI access to running playbooks

© 2018 Cisco and/or its affiliates. All rights reserved.
Automating Peering Changes
Cisco Peering NSO Automation

- Peer Management
- Peering Telemetry Deployment
  - Deploys peering-specific telemetry
- Peering ACL Deployment
- Peering AS-Set and Prefix-Set Deployment
- Peering Route-Policy Deployment
- Netflow Enablement
- Maintenance “drain” automation for Peering nodes
- Peering Fabric node management
  - Addition of PFL nodes configures all PFS nodes

Deployment services can load templates with pre-defined policies or allow the creation of new elements for deployment to peering nodes.
Cisco Secured Intelligent Peering Solution

**Trusted and secure portfolio**
- Trusted platforms with SW run time protection
- Cloud powered BGP security monitoring
- DDoS protection

**Intelligent**
- Optimization tools help enhance services
- Simplified design with traffic engineering

**Cost optimized**
- Distributed peering reduces transport costs
- Flexible Consumption Model with pooling of capacity
- License portability provides investment protection

**Power / space optimized**
- Highest density in optimized form factor
- 20% lower power compared to leading competition
- Lower Total Cost of Ownership (TCO)

**Software driven**
- IOS-XR with enhanced BGP protocol stack
- Automation focused
- Open API driven / Programmability
- SDN driven Framework

© 2018 Cisco and/or its affiliates. All rights reserved.