The Chartered Institute for IT

Enabling the information society

SD WAN 101

BCS Northamptonshire Branch

Date: Tuesday 10th December 2019

SD WAN 101

Barney Duffy
FBCS CITP, MIET, MACM

Agenda

- SD WAN what is it?
- Benefits of SD WAN
- Comparing MPLS, Which is better
- Cloud based solutions
- Hybrid Solutions
- Considerations before you deploy
- Where is the technology going
- When is the right time.

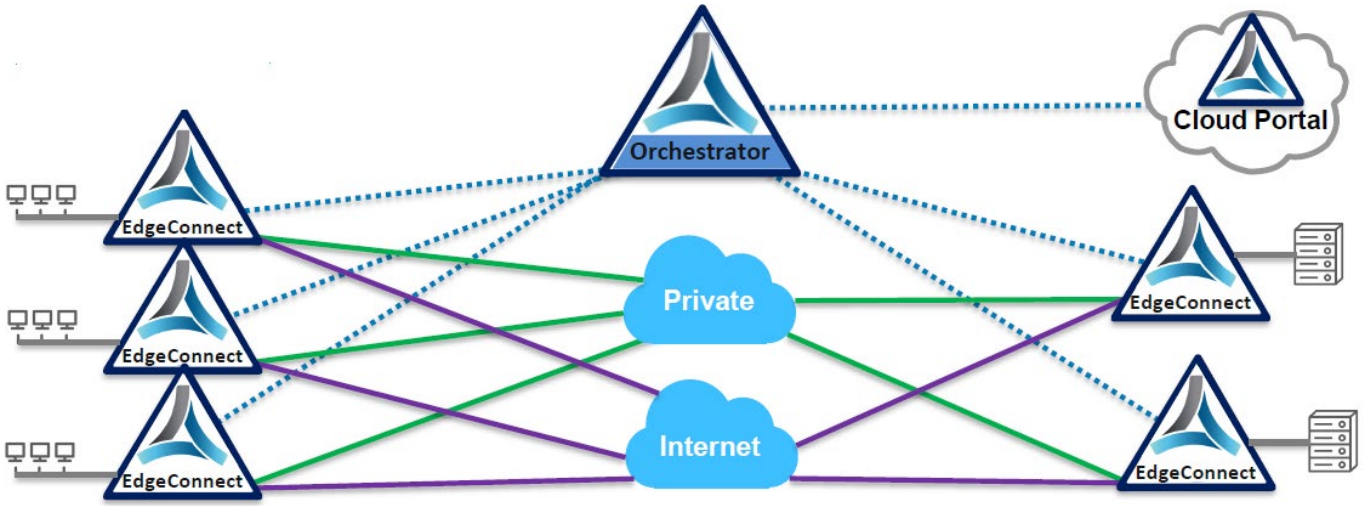
What is SD WAN!

- SD-WAN is an overlay service that can be delivered over any IP routed underlay network, including MPLS, Wireless, Mobile and Direct Internet Access (DIA). It can bond mix of Underlay e.g. Internet, 4G, MPLS (hybrid)
- SD-WAN delivers application routing, efficient offloading of expensive circuits, and simplification of WAN network management. It Splits the Control Plane from Data Plane.
- SD WAN Primary advantage is security. SD WAN deploys end to end security across the network. All devices and endpoints are completely authenticated (Scalable key exchange functionality and Software Defined Security)
- Multiple Connectivity Options! Such as;
    - Hub Option based on a number of sites using small bandwidths such as FTTC deploying a central controller to mediate all of the tunnels and routing e.g. an SD-WAN controller is operationally easier than SAs & routing on box basis via CLI.

What is SD WAN!

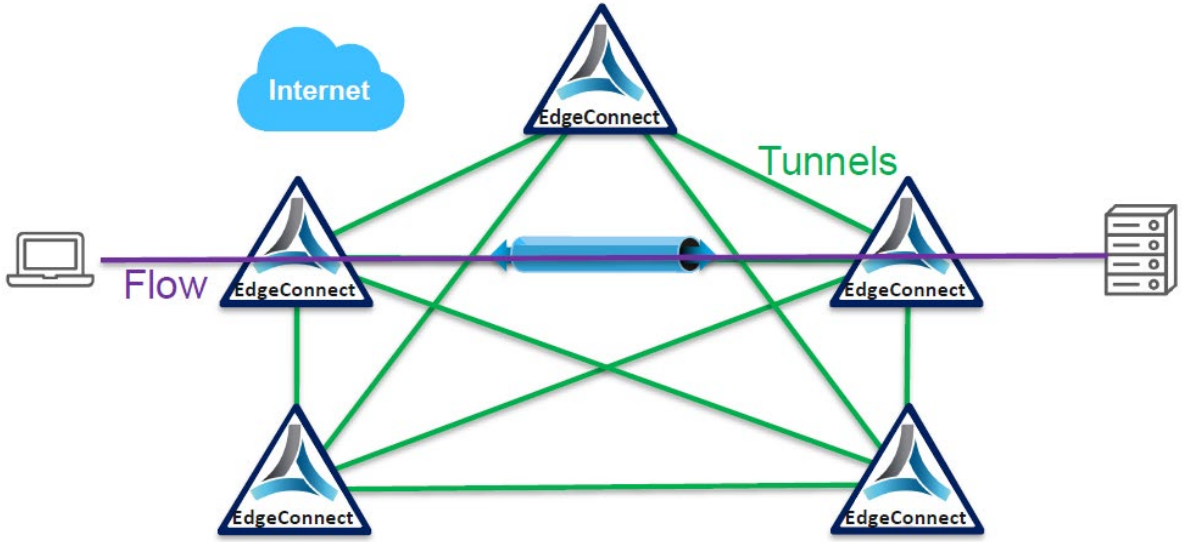
- Software Defined Networking (SDN Orchestration)
    - The ability to automate behaviours in the network. Co-ordinating hardware and software to support applications and services. Requires User and Application profiling.
    - Regular updates to network configuration.
- **Considerations**
- SD WAN is able to control the route between sites where multiple paths exist, The network is monitored for delays. However on a single link this is restricted, especially if the bandwidth is limited.

SD-WAN Components



- **EdgeConnect Appliance** – Transports and optimizes traffic between sites in the network
  - **Physical Appliance** – Hardware that comes with software loaded and a burned in serial number linked to an account
  - **Virtual Appliance** – Software appliance running in a hypervisor. No serial number - requires license info to link to account
- **Orchestrator** – Manages, provisions and monitors the Silver Peak devices in a given network.
  - Must register with the Cloud Portal to manage EdgeConnect appliances.
- **Cloud Portal** – Silver Peak's portal on the internet.
  - Manages licensing of Silver Peak devices in a network. Talks to Orchestrator and EdgeConnect devices. Knows all licenses and serial numbers of physical devices. Facilitates initial connection between Orchestrator an Edge Connect devices. All devices must register with the Cloud Portal.

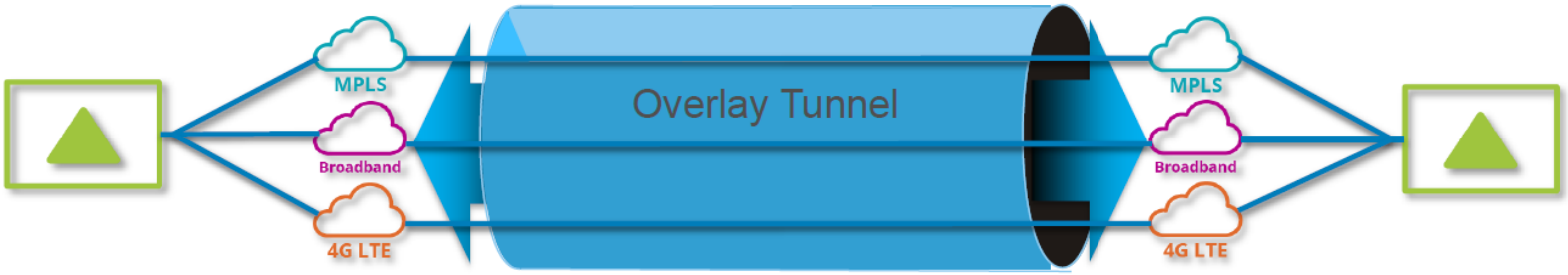
Flows



- **Flow** – A stream of packets transmitted between two endpoints
  Usually identified by at least a Protocol, Source Address and Destination Address (and possibly source & dest port numbers). May or may not be tunnelized.
  - **Stale Flow** – A flow that existed prior to a configuration change on a Silver Peak that is operating under old rules.
    - E.G. A policy change is made after a flow has already been established
    - **Note:** *In current software, flows are automatically **reclassified** every minute. This may correct many issues, but it does not **reset** a flow (send an RST). A flow reset may be required after certain configuration changes.*

Underlay and Overlay Tunnels

- **Underlay Tunnels**
  - The physical transport network and its site to site connections built using IPSec_UDP* tunnels. Could use MPLS, Internet, LTE or other transports
- **Overlay Tunnels**
  - Logical connections that make use of one or more underlay tunnels. Data can be distributed across multiple underlay tunnels using multiple transport methods depending on configuration



* IPSec UDP is the default. Other tunnel types are supported

Benefits of SD WAN

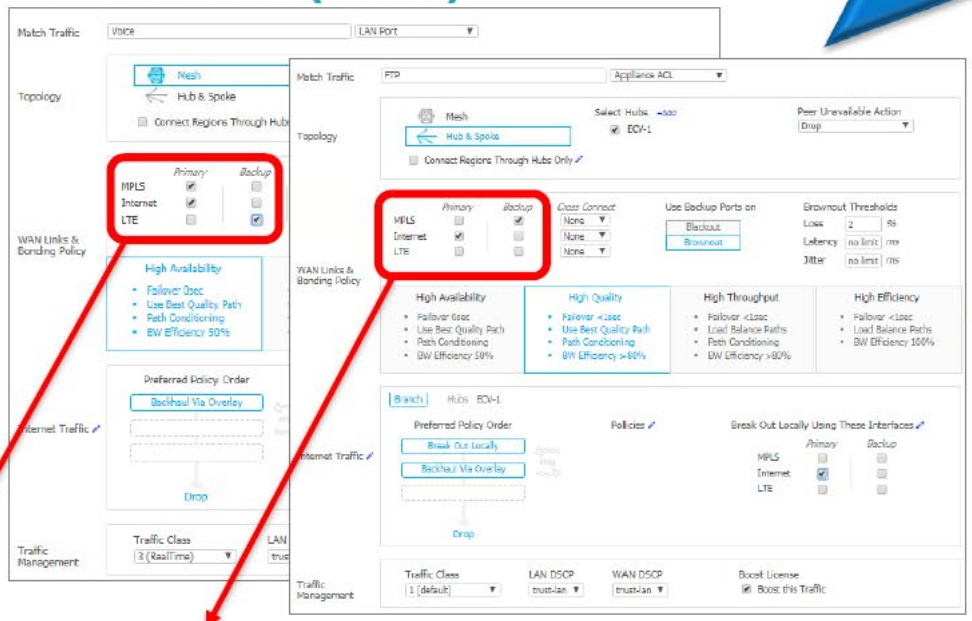
- Visibility, Flexibility and Control.
- Rapid Deployment using a range of connectivity options.
- Can be cheaper than a fully implemented MPLS WAN (The internet is not universally cheaper than MPLS (especially in the UK))
- Easier to Manage and Update the network using Automation Reducing mistakes.
- Ability to load balance across Primary and Secondary Circuits saving against more expensive fibre circuits. (Deliver better performance from twin circuits)
- Application integration into SD WAN Orchestration allowing intelligent management of Applications. (Real-time application routing)
- Improving performance of Cloud services such as SaaS and IaaS by using virtual devices.
- Add Consistency by deploying Template designs across sites.
- Reduce administrative costs for the networks especially Moves and Changes.
- Useful metrics and reporting (Analytics)

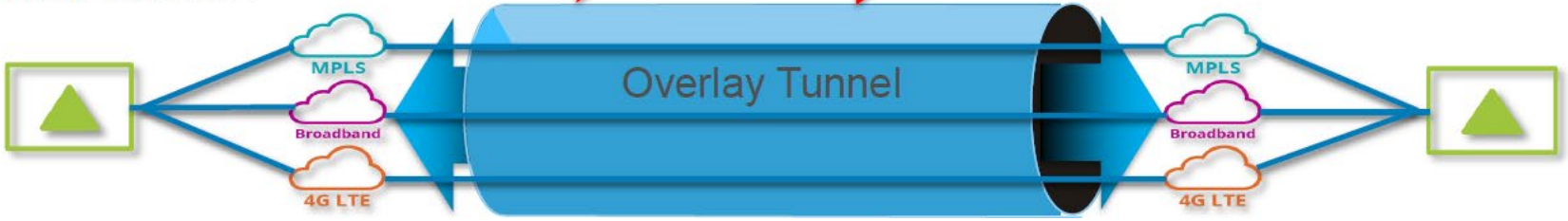
Business Process

BUSINESS INTENT OVERLAYS (BIO)

More than one BIO can use the same underlay tunnels in different ways

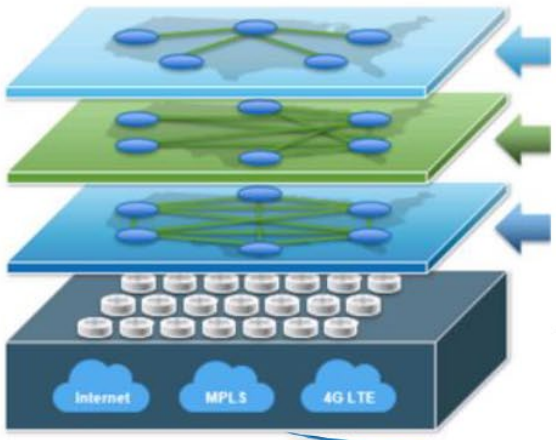
- The set of policies and configuration parameters that determine:
  - Which transports are used for underlays
  - Which underlays are used for each overlay
  - How the traffic is distributed across the underlays
  - And more…





A SOFTWARE DEFINED WAN (SD-WAN)

MULTIPLE BUSINESS INTENT OVERLAYS



Overlay Name	Topology	Underlays	Boost?	Internet Traffic	Goal
Guest Wifi	Hub & Spoke	Internet	No	Backhaul →Zscaler	Cost Savings
Critical Apps	Mesh	Internet MPLS 4G LTE*	Yes	Local Breakout	Maximize Quality
RealTime	Mesh	Internet** MPLS** 4G LTE*	No	Zscaler	Maximize Availability

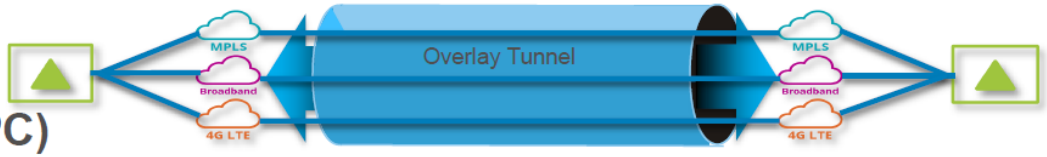
Each Overlay is created by a different BIO with different characteristics

* Backup
* * 1-1 FEC (Better than mirroring)

Underlay & Overlay tunnels:
Physical Transport Networks & Logical connections

FEATURE TERMINOLOGY AND DEFINITIONS

- **EdgeConnect Basic Features**
  - **Path Conditioning**
    - **Forward Error Correction (FEC) –** Uses parity packets to reconstruct lost packets to avoid retransmission
    - **Packet Order Correction (POC) –** Reorders any out-of-order packets to avoid retransmission

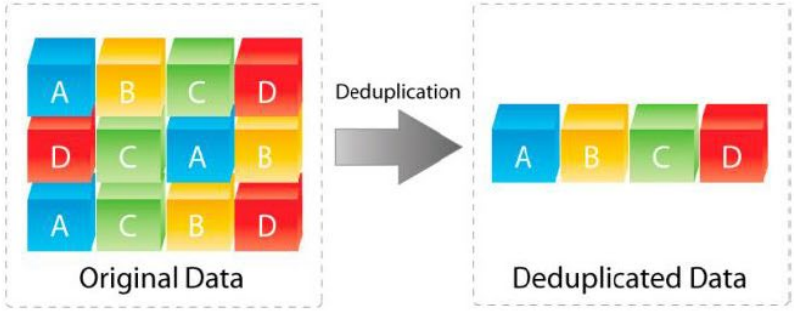


  - **Dynamic Path Control (DPC)**
    - Dynamically select the appropriate underlay tunnel
      - 1-1 FEC (HA)
      - Choose tunnel based on Quality – loss, latency, jitter (HQ)
      - Load Balance (HT, HE)

Network Optimisation Technologies

– FEATURE TERMINOLOGY AND DEFINITIONS

- **BOOST** = WAN optimization technologies available as an extra cost option
  - **TCP Acceleration –** Optimizes the TCP protocol to mitigate the effects of latency
  - **Network Memory –** Deduplicates transmitted data to reduce congestion



Application	<-- Reduction %	<-- Bytes	Bytes -->	Reduction % -->
Cifs_smb	83.1	289G	49G 17G	289G	94.1

Comparing MPLS, Which is better

Both technologies have their Pros and Cons

MPLS

- If it is a straight forward comparison then MPLS has its routes in the past and works well with older technologies.
- MPLS network equipment is interchangeable because of standards
- Core Firewall services (Single point of Failure against Simpler management)

SD WAN

- SD-WAN has its routes in the future, however we are not there yet as far as standards. (This area is work in progress)
- SD-WAN is very good at Cloud based solutions, this also includes Private Cloud.
- SD-WAN is very good at Automation.
- Cloud based Firewalls, Local Proxy Firewalls plus Centralised Firewall Services
- SD WAN can make WAN Optimisation easier and cheaper to deploy

Hybrid

- This is where SD WAN is applied to MPLS circuits (Easy to Migrate)

Cloud Based Solutions

- SD WAN improves Cloud Application performance by measuring the best route and allowing for local internet breakout.
- Companies are migrating to Cloud based applications such as Salesforce or Microsoft Office 365. In a standard MPLS network, traffic has to traverse a central firewall at the HQ requiring more bandwidth at the HQ to trombone traffic in addition to increasing latency.
- SD WAN allows remote sites to access Cloud applications via the Internet. This will provide a shorter path improving performance. it will also reduce the MPLS loading.
- Cloud platforms such as AWS and Azure have the option for Private Cloud Connectivity (Hosted Applications that have been migrated to the Cloud Platform). This allows branch sites to reach the IaaS platform and should have a better SLA. Performance depends on geography - which region the Branch site and the IaaS platform reside in. Generally this provides a cost effective, high performance connection through the Cloud Gateway.
- SD WAN makes Cloud Based Applications easier to administer and secure. SD WAN uses URL and DNS to keep track of changing IP addresses by using the URL and DNS. Updates to IP Addresses will automatically update the SD WAN device.
- With a traditional WAN, one has, periodically, to update the IP Addresses that the firewall will allow inbound traffic from; otherwise it may block O365 traffic.

Hybrid Solutions

Benefits

- A hybrid WAN enables the use of both SD WAN and MPLS technologies. Deploying a Hybrid solution allows the shared use of both MPLS and Internet circuits.
- Deploying SD WAN on an existing MPLS Network allows intelligent path selection in real time across the WAN. (Dynamic Multi-Path Optimisation DMPO)
- Users are guaranteed the best network connectivity when they access Cloud based applications from anywhere on the network (Without deploying QoS)
- There is improved visibility and control of Traffic Routing, Performance and Policy management.
- Hub and Spoke Type deployments.

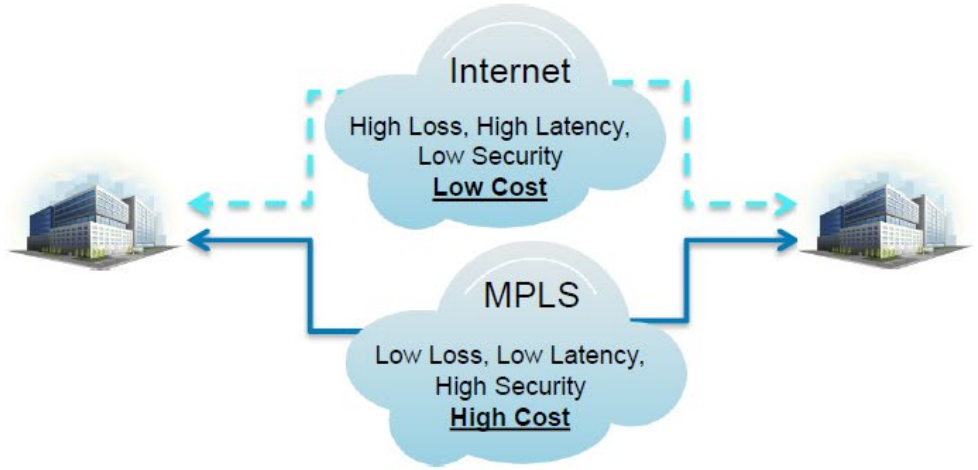
Hybrid WAN

THE WAN IS CHANGING

CUSTOMERS MOVING FROM MPLS TO HYBRID MPLS/INTERNET OR DUAL INTERNET FOR WAN

Traditional WAN

Hybrid WAN



Courtesy of Silver Peaks

Considerations before you Deploy

- Pick the right vendor as you cannot mix SD WAN vendors on a single WAN.
- The biggest inhibitor for SD-WAN is it's new and that standards for SD WAN are not complete
  - SD-WAN uses traffic steering that varies from traditional methods this is what gives it flexibility.
- Policies need to consider the Network and the Application. This means understanding Business Requirements, how the applications works, and how the network will handle the traffic.
- Understand your business model. Identify mission critical applications and functions. Understand how the SD WAN will integrate into your existing network. (Hybrid)
- Thoroughly test the Network and the Applications before Deployment. Don’t cut corners.

Private Cloud Applications.

- The complexity comes because the Application Development Team and the Network Engineers need to ensure both the Network and Applications are co-ordinated to enable the network layer to meet application requirements. This is where integrated analytics can help detect any issues. These features need to be built into the applications.

Where is the Technology Going

- Improved Security on the WAN.
- SD-WAN is a Networking Technology that decouples networking hardware from its control mechanism.
- It's the migration of Physical Network Hardware to Virtual Applications that may reside on the same Virtual Appliance as the Applications. (Or even be part of the Applications)
- The core aspect of SD-WAN is a control mechanism that intelligently directs traffic across the WAN to improve the overall application speed and performance.
- SD WAN handles traffic based on Policy (Priority and Security)
- Currently SD WAN Integrates with Applications, eventually SD WAN Technology may become part of the application.
- MPLS technology will not be replaced overnight, there will be a requirement for a few years yet to come.
- Reduction in Network Opex Costs.

When is the right time to Deploy.

- This will depend on where you are.
- **Considerations**
  - How dependant is your company on its Network and Applications
  - Where does your Company stack against its competitors in the deployment of such technologies.
  - Current Network infrastructure
  - Current Application Build
- Trying to run older mainframe applications on an SD WAN will not benefit from the network infrastructure. This is where Hybrid comes in.
- Do you have a good Application Development team with experience in this area.
- Has your team good knowledge in Application Testing and Deployment.
- Can you purchase Opensource Applications that can be modified to suit your needs.
- Do you have a sound Network team with experience of deploying this technology.
- If not then you need to consider building a team.

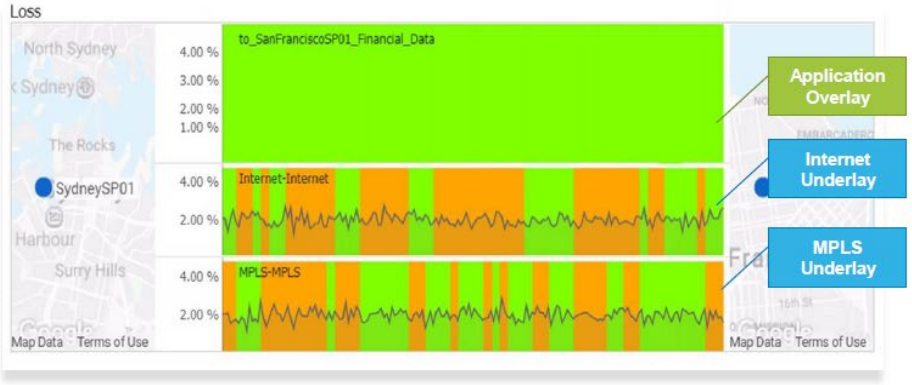
Application Management and Control

APPLICATION SLA ACROSS ANY TRANSPORT

Increase user productivity and satisfaction

Predictable, non-disruptive application performance even during transport brownouts or outages

- Tunnel bonding
- Path conditioning
- Packet-based load sharing



Silver Peak Live View monitors network underlay and application overlay performance in real time

Courtesy of Silver Peaks

Thank you

BCS Northamptonshire Branch

Thank you for attending!