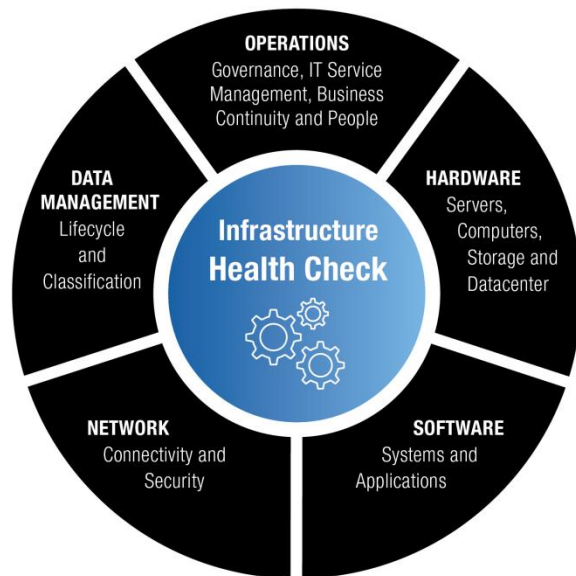


IT Infrastructure Health Check

Vandelay Industries infrastructure assessment



ADVISORY SERVICES



This report was prepared by WG Advisory Services for the Vandelay Industries on June 1st, 2017

The information in this report is based on the Infrastructure Health Check (IHC) framework co-developed by WG Advisory Services Inc. Ratings contained in the report were established using a range of subjective tools (interviews and surveys) and detailed technology analyses using a combination of software tools and infrastructure reviews by subject matter experts (SME).

Completion Rate

100%

NETWORK SCORECARD

OVERALL RATING

Overall Health Check Rating is based on the rolled-up score of all areas defined within Network: Network Infrastructure Architecture, Network Management, and Connectivity.

IT Infrastructure Health Check: Network
May 16th, 2017

Last Year	Architecture – Management – Connectivity	Health Check Rating
N/A		2.2

NETWORK INFRASTRUCTURE ARCHITECTURE

VALUE SCORECARD
NETWORK

RATING LEVELS	NETWORK ARCHITECTURE	 MEETS NEEDS	 RELIABILITY	 OBSOLESCENCE	 COST \ EFFORT
3 HIGH	Network Roadmap				
2 MEDIUM	Performance Capacity Planning				
1 LOW	Operating Procedures				

ITEM	CURRENT RATING	PREVIOUS RATING
NETWORK ARCHITECTURE	1.6	N/A

Synopsis

The network infrastructure at Vandelay outside of WREPNET, is managed by too few individuals with most of the knowledge retain by the individuals rather than documented in SOPs and operational standards.





Due to the lack of a SOP framework, documentation standards and a reference architecture, decisions to build and expand Vandelay network infrastructure have mostly been ad-hoc and 'stop gap' based.

Over the years no formal network architecture is developed, changes to the infrastructure have been dealt with by point solutions, creating a dispersed and 'island-based' landscape of tools, technology and a multitude of vendors.

The cost to maintain the Vandelay network infrastructure is high, in financial terms, as well as in the workload on a few individuals and the risk of losing knowledge without proper documentation. The lack of an best business policy practices such as an IP address scheme, Configuration Management DB, vendor management, naming convention, network documentation and diagrams, makes every change, outage and build-out become a challenge with high risk, stress, dependency on individuals, unnecessary long lead times and high cost to the organization.

CONNECTIVITY (LOCAL AREA NETWORK)

VALUE SCORECARD
NETWORK

RATING LEVELS	LOCAL AREA NETWORK	 MEETS NEEDS	 RELIABILITY	 OBSOLESCENCE	 COST \ EFFORT
3 HIGH	WIRED NETWORK				
2 MEDIUM	Wired Layer 2				
1 LOW	IP Address Scheme				
	Naming Conventions				
	VLAN Scheme				
	Core as L3				
	QoS (Business Applications)				
	QoS (VOIP\Video)				
	WIRELESS NETWORK				
	Separate SSIDs				
	Wireless Security				

ITEM	CURRENT RATING	PREVIOUS RATING
LAN	2.8	N/A

Synopsis

The network infrastructure at Vandelay outside of WREPNET, is managed by too few individuals with most of the knowledge retain by the individuals rather than documented in SOPs and operational standards.

Due to the lack of a SOP framework, documentation standards and a reference architecture, decisions to build and expand Vandelay network infrastructure have mostly been ad-hoc and 'stop gap' based.

Over the years no formal network architecture is developed, changes to the infrastructure have been dealt with by point solutions, creating a dispersed and 'island-based' landscape of tools, technology and a multitude of vendors.

The cost to maintain the Vandelay network infrastructure is high, in financial terms, as well as in the workload on a few individuals and the risk of losing knowledge without proper documentation. The lack of an best business policy practices such as an IP address scheme, Configuration Management DB, vendor management, naming convention, network documentation and diagrams, makes every change, outage and build-out become a challenge with high risk, stress, dependency on individuals, unnecessary long lead times and high cost to the organization.

APPENDIX A: NETWORK – MANAGEMENT

IP ADDRESS MANAGEMENT (IPAM)

The IP address scheme at Vandelay is currently a work in progress. The work entails the migration from public address space to a private space.

We support this move entirely.

Important to emphasize here is that there is more to moving from public to private space than a simple replacing IP numbers. A solid and well-orchestrated IP scheme is vital to any network infrastructure.

During the assessment we discovered that the migration is not yet completed and that the public and private IP addresses are used in and between locations, as the screen shots below shows.

We compiled the distinct subnets from the routing table as reported in Solarwinds and removed duplicates. Based on the 508 unique IPs reported, 101 are public IPs in use.

Access provisioning to our performance monitor was also provided using a public facing IP, allowing for (too) easy access by other parties than our consultants.

Conclusions & Recommendations

The key to a manageable and expandable IT infrastructure is to have a consistent Layer 2 with easy to understand Layer 3 structure across all Region locations. This allows for a uniform level of network connectivity services, fair or equal distance between resources and additionally more bandwidth to each building whilst maximizing the use of IP address space to facilitate a highly functional and easier to manage Local Area Network. Vandelay is as complicated as any public service provider or major enterprise in and of itself and needs the same level of consideration those entities rely on for their IT needs.

In order to obtain this goal, the following is required as part of any architectural design change:

- VLAN/Subnet Segmentation
- Additional UP/DOWN Link network segments to be created
- Redesign the Core/Distribution/Access layer
- Investigate the possibilities of reusing existing equipment as part of the new redesign
- Reconfigure existing equipment into the first Core, Distribution, and Access layer topology using existing equipment for now.
- Change the core router (switch) configuration to reflect the needs of the new design.
- Ultimately establish the future campus-wide topology hardware selection

Designing an IP scheme requires applying a number of best practices, well documented and rigorously adhered to policies and procedures.

Below a sample of an internal (10.x.y.z) private network, using a structure approach of using the last three octet (.x.y.z) to reflect function, location and destination.

NetworkID	Q4	SubnetBits	VLANID	Purpose	Description		
10.101.	0	16	n/a	SiteLevelNetworkAssignment	PrimarySubnetTiedtoStreetAddress,SiteCodeorCombinationandFull6bitsofallocationpotential		
10.101.1	0	24	1	LANMGMT	Allswitches,routers,waps,firewallsfornormalandoutofbandmanagement	VLAN101.1.0/24	LANMGMT
10.101.3	0	24	3	PUBLICOUTSIDEPRISWITCHINTUNUMBERED	FirstVLAN(perInternetLink)foruseinbutsideoffirewallandbetweenfirew	VLAN101.3.0/24	PUBLICOUTSIDEPRISWITCHINTUNUMBERED
10.101.6	0	24	6	DMZ(includinginsideLANgear)		VLAN101.6.0/24	DMZ(includinginsideLANgear)
10.101.10	0	24	10	CORESWITCH3PEERING		VLAN101.10.0/24	CORESWITCH3PEERING
10.101.11	0	24	11	CORE1toFW1U/L		VLAN101.11.0/24	CORE1toFW1U/L
10.101.12	0	24	12	CORE1toFW2U/L		VLAN101.12.0/24	CORE1toFW2U/L
10.101.21	0	24	21	CORE2toFW1U/L		VLAN101.21.0/24	CORE2toFW1U/L
10.101.22	0	24	22	CORE2toFW2U/L		VLAN101.22.0/24	CORE2toFW2U/L
10.101.51	0	24	51	SERVERFARMMGMTIBMBBladeCenterS			
10.101.52	0	24	52	SERVERFARMMGMTIBMBIMM			
10.101.53	0	24	53	SERVERFARMMGMTIBMBIDRAC			
10.101.54	0	24	54	SERVERFARMMGMTIBMBNon-Server			

Recommendations

The diagram below shows at a high level how Vandelay infrastructure campus-wide could be. Taking into consideration a consistent model that can be applied to any location of any size.

Considerations

Legacy equipment and bandwidth considerations should be explored to determine the best and most complimentary hardware and software that Vandelay can deploy.

The standard model proposed above shows virtually all links in an active/passive state. Perhaps Vandelay is ready for the next generation networking technologies granting shorter ROI, increased equipment and product feature longevity with reduced operational cost while simplifying operations. This model supports that and in fact may reduce the number of new devices and relative complexity in some cases.

This design incorporates all the modern methods required to deliver predictably better performance to everyone RoW IT supports. A fairness policy could be established whereby application performance can be tuned, improved and accelerated for every flow over school networks. This means the same level of expectations and performance could be experienced by staff, students or faculty from any of your locations including those not on the MPLS, on the Internet or through site-to-site VPN tunnels.

By moving towards an enterprise private IP based network design with consistent equipment, topologies and naming conventions, RoW would be able to concentrate on bigger projects, application specific improvements, and business drivers of the organization.

No network administration should be created that makes it harder to support than it should be. A multi-stage and multi-layer ITIL management design can be incorporated into this design with ease facilitating the ability to move away from locked areas of the network that cannot be administered in the same ways as others. No more VPNs to support devices hidden from view and all devices should be visible to IT management tools.

We would like to recommend beginning to entertain the concept that despite Vandelay having public IP addresses, ISIT has the choice to simply not operate like the public Internet and bring back control, predictability, performance and consistency to the IT teams that service the remainder of IT and the entire user community.

CONFIGURATION MANAGEMENT DATABASE (CMDB) - NETWORK MANAGEMENT SYSTEM (NMS)

During the Assessment Phase of this project it became apparent that most information is stored inside a limited number of individuals memory, rather than in a management system.

Not having immediate access to accurate network asset information puts any support and service desk in a disadvantage.

It also limits Vandelay's support organization to dispatch other support team members to fix or support on a call, since the information is only available to a person, not a shared repository. A good example is the network topology diagram of the Frederick Street network (below). Not only incomplete in the exact number of network elements, it contain old and missing information.

This example highlights a few or several missing NSM essentials:

- No Consistent IP address scheme, using self-explanatory convention
- No Accurate representation of today's network
- No interconnecting devices leaving this diagram to a next level diagram
- No IP relationship to Device Naming
- No use of symbols
- No date/author/reference

When logging into the Solarwinds NMS, information was not always available to view, as the screen shot below shows. This may be related to a missing Netflow feed, however a lot of network metrics is available on all devices and should be embedded in the NMS.

Recommendations

- All of the above, and much more, can be avoided by using SOPs with support of a Network Management Systems (NMS).
- As much as Vandelay has Solarwinds deployed, the system is not used to its maximum capacity and capability.

- This is not to be said that Solarwinds can do all of the functions, hence our recommendation to 'look before leaping' into "buying more".
- Essential first stage of requirement gathering is to identify which disciplines of an IT Support organization are going to use the NMS and for what purpose.

Not only should an NMS system, like Solarwinds poll devices to get information, it should:

1. Have event/log consolidation and cross-correlation spanning network, system, application, directory, access, identity, location, and physical sources.
2. Discover changes to the infrastructure, access to trending and topology mapping
3. Track changes, validation and audit
4. Perform Network behavior analysis
5. Record Network inventory: devices, systems, and applications, with location information.

Not having these basic NMS functions in place makes every change, outage and build-out become a challenge with high risk, stress, dependency on individuals, unnecessary long lead times and high cost to Vandelay.

Vandelay needs a network management framework, using ITIL as guidelines to identify improvements to service, automate operations, align network to business priorities and to work towards monitoring by exception instead of firefighting. Adopting a number of ITIL based practice areas will allow Vandelay to quickly enable SOPs in this NMS and other areas.

LOCAL AREA NETWORK (LAN)

WIRED LAYER 2 – VLAN SCHEME

The wired layer 2 and VLAN network infrastructure has a robust VLAN structure in place. The WREPNET VLAN is 600 as 'root' of the VLAN scheme. The internal (Frederick Street) network infrastructure has a further VLAN break-down to business functions and services.

In review the VLAN documentation, we discovered several anomalies in the listed VLANs. This caused some confusion and rectifications on the list whilst in the meeting. Whilst this is not uncommon, it does highlight the risk of improper documentation and risk of error during troubleshooting and fixing issues

As much as the VLAN had a reasonable documentation in place, the actual layer 2 network topology was very poorly documented, as the sample below shows.

This diagram has many flaws.

- Having question marks in an IP address indicates that there is no further documentation available

- During conversations, it turned out that some of the IP in this diagram and subnets are wrong or incomplete
- When troubleshooting, following this diagram will be of very limited help to fix.

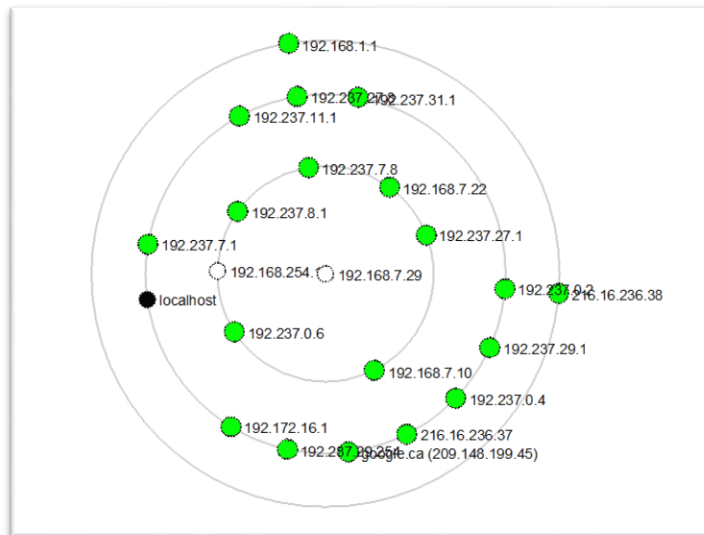
As we needed a common reference diagram during the project, we created a top-down structured Visio diagram for discussion purposes in the meetings. Below a sample of a brief effort of restructuring the previous diagram:

This more structured visualization, allows for a quick 'walk-through', easy identification of elements and their dependencies.

Conclusions

Improper documentation and not using best (ITIL) practices in documentation, updates and use of structured methods, leads to long mean time to repair, unnecessary down-time, loss of credibility and end-user confidence.

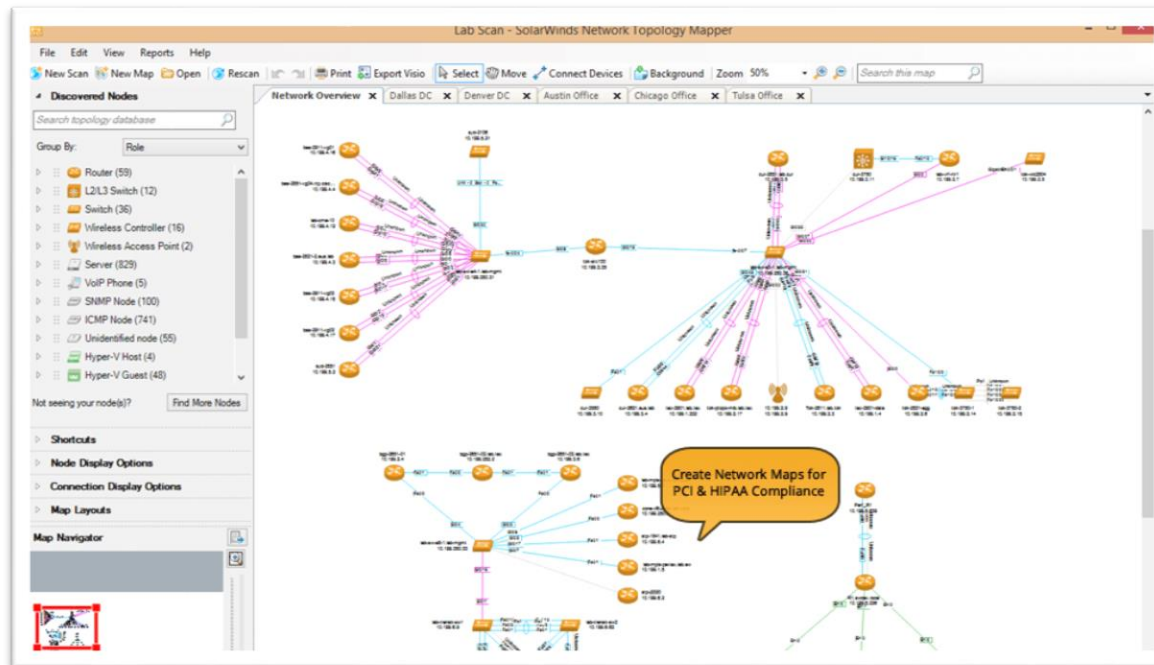
Having several views, documents such as the above, combined with access to instant dependency-views like the example below, allow for faster trouble shooting, root cause analysis. The same elements in the Visio diagram are shown here, in a layer 2/3 routing tree, live from Vandelay's network.



The Visio diagram above is a first steps towards documentation, which will have to include logical diagram sections, separating business services by means of color schemes and functions.

Based on our findings, we highly recommend:

1. Properly document the layer 2 and 3 network topologies of all main locations
2. Use of industry standard tools, allowing to export, edit and maintain documents rather than using a simple drawing tool and PDF
3. Investigate the use of Solarwinds' Network Topology Mapper that allows for real-time and up-to-date network topology maps



WIDE AREA NETWORK (WAN)

WAN BANDWIDTH MONITORING

The current 1G and 10G bandwidth connection are deemed to be sufficient for the internal data transfers. We have not heard the interviewees mention any pressure on users complaining about slowness of their applications.

What we've also not heard is how the VI-IT team prepares for the future development of the overall network infrastructure. There appears to be limited urge (and time no doubt) to anticipate on performance and capacity planning. Inside ITIL a crucial component of any ITSM SOP.

Since Solarwinds' dashboards are empty (when using our accounts) it remains unclear if and how this platform is used for planning purposes or merely for troubleshooting.

WAN QoS

In the context of WAN, we refer to the WREPNET as WAN. On this network a single VLAN 600 handles all RoW internal traffic, and only VoIP has a priority tagging. This means that all other traffic, such as VPN coming from Maple Grove to Frederick, data backups, application access and DR are all sharing the single traffic lane, all competing for access.

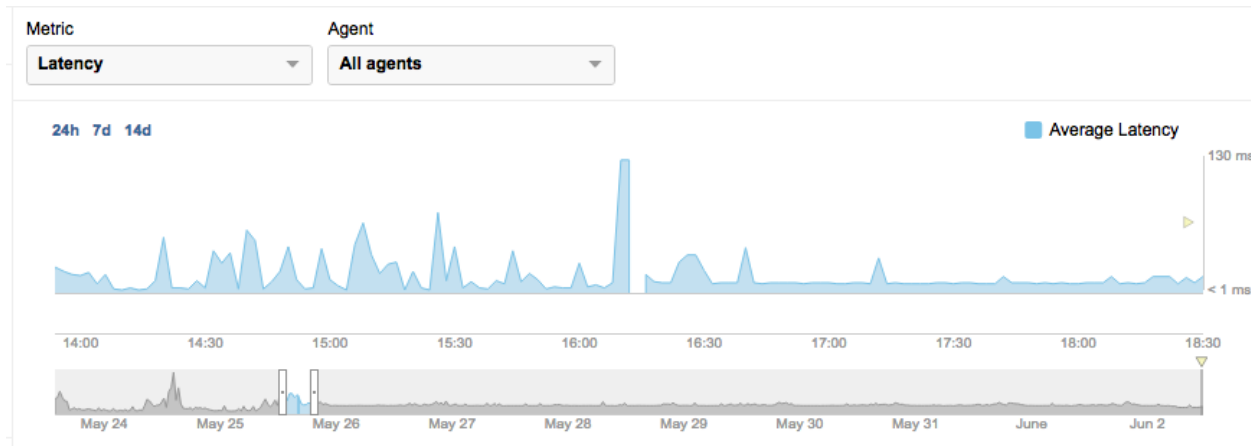
As much as 10Gbps allows for many flows to use this highway, it remains good practice to tag data based on priority, maximum allowed usage and time-of-day usage. Networks like shown in the diagram below are even recorded by us with 1GBps+ networks.

The 10G interconnect is provided by SoftChoice. Based on the Monthly Vitals reports we received, there is no capacity/bandwidth chart available, only down-time statistics.

Device Availability					
Availability Achievement by Technology					
Technology Group				Actual	Target
Network				99.967 %	99.900 %
Top 10 Lowest Availability by Device					
Device Name	Top 5 Outages			Actual	Target
RMOW_50_QUEEN	Outage Start	Outage End	Outage Duration	97.807 %	99.900 %
	3/15/2017 7:49:33 PM	3/16/2017 12:08:33 PM	16 Hours, 19 Minutes		
	1 Outages with a Total Duration		16 Hours, 19 Minutes		
WRDSB_WESTHEIGHTS	Outage Start	Outage End	Outage Duration	97.883 %	99.900 %
	3/6/2017 3:40:27 PM	3/7/2017 7:25:27 AM	15 Hours, 45 Minutes		
	1 Outages with a Total Duration		15 Hours, 45 Minutes		
WRDSB_SHEPPARD	Outage Start	Outage End	Outage Duration	98.286 %	99.900 %
	3/17/2017 6:09:34 AM	3/17/2017 6:54:34 PM	12 Hours, 45 Minutes		
	1 Outages with a Total Duration		12 Hours, 45 Minutes		
COK_CAMERON_HEIGHTS_POOL	Outage Start	Outage End	Outage Duration	99.272 %	99.900 %
	3/15/2017 9:28:33 AM	3/15/2017 2:53:33 PM	5 Hours, 25 Minutes		
	1 Outages with a Total Duration		5 Hours, 25 Minutes		

INSIGHT INTO BUSINESS APPLICATIONS VS. RECREATIONAL

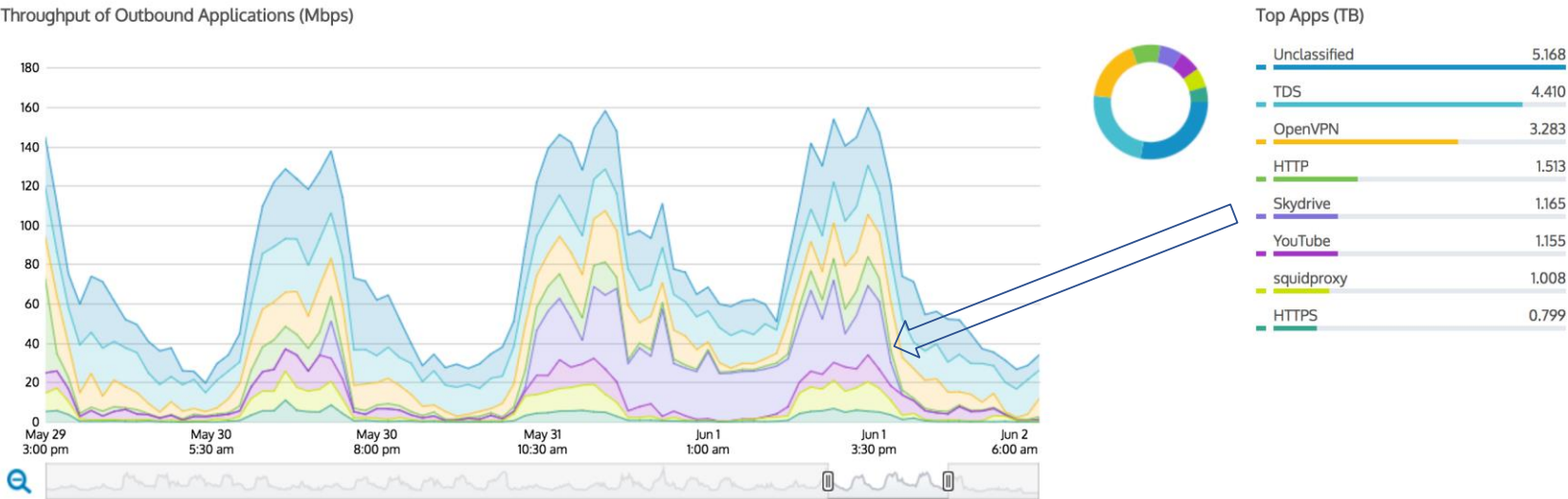
As part of every network assessment, we active an application monitor that tracks real-time traffic on the infrastructure (without storing any payload or user content). During this assessment we installed the monitor on the Internet connection between Frederick Street and Vandelay's Internet provider. Initially this was a 100 Mbps until May 25 when it was upgraded to 1Gbps. The switch-over we recorded in one of our monitors.



Interesting difference between before the switch over and after is the higher noise level of latency.

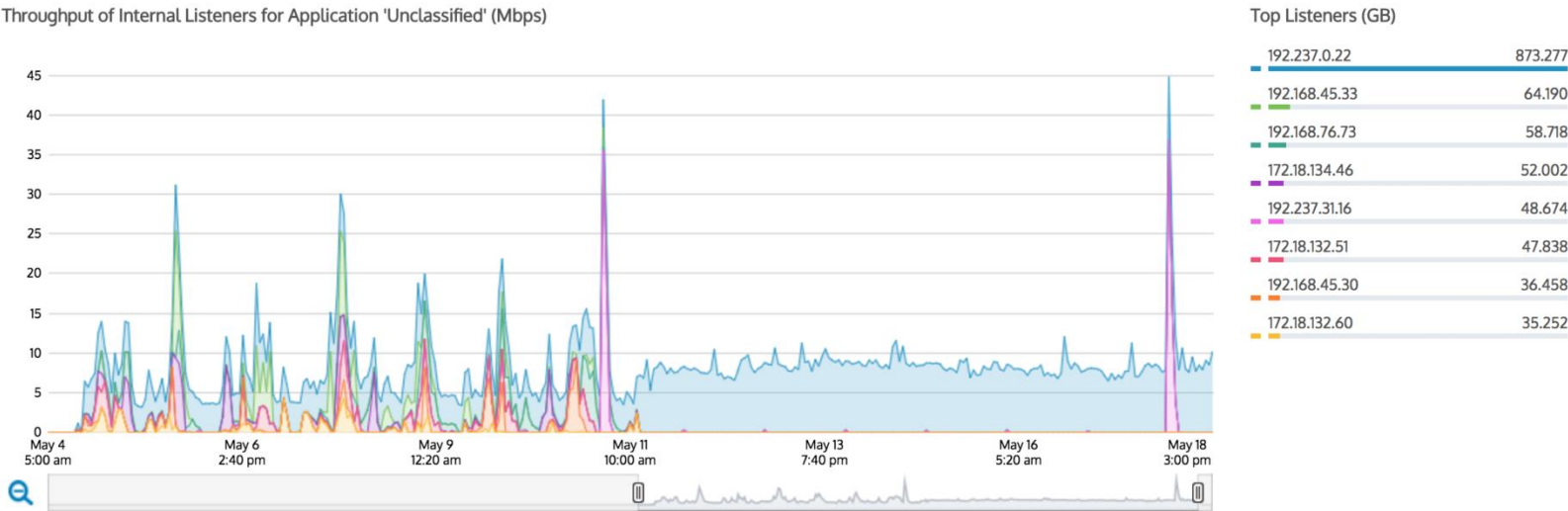
The actual traffic on the Internet connection was as we would expect on any unmanaged Internet connection. 60-80% recreational use.

Most of the traffic is originating from the Meru Wi-Fi controller and the Barracuda Webfiler appliance. On several occasions, including 1st week, we did notice a large data transfer outbound from an internal user/process to Microsoft's OneNote (Skydrive) is over 450 GB.



This may be a legitimate process uploading documents, however, given the infrequent nature during our 30 days measurement period, it could be a potential security risk (DLP).

Another observation was a sudden change in traffic flow/conversation on/after May 11th:



Data that was until May 11 destined for leaving the network across the Internet was no longer recorded, or masked (higher light blue graph from May 11 onwards. The light blue is data originated from the Meru controller.

Conclusions & Recommendations

In the context of QoS, performance monitoring and capacity planning, it is in our expert opinion essential to utilize and/or implement performance and capacity monitoring solutions.

These dashboard-type solutions with real-time data give immediate insight into the current state of an infrastructure and allow to act preventively rather than in a reactive mode.

These monitoring solutions enable Vandelay's IT to plan ahead of any change, evaluate application load, data storage patterns and protect existing end-user performance SLA.

Sanctioned vs. Shadow IT¹

In light of more and more services and applications being offered on the Internet, end-users see and feel no boundaries any more on sharing, posting and storing data into the Cloud. This causes major security concerns to many organizations. With more than 22,000 cloud services available, chances are that Region employees are using between 150-200+ of these services.

Some are innocent such as YouTube and Facebook, others are less, whereby data stored on these services are copied to malicious servers and invested with ransomware and posted back on the users domain.

We recommend Vandelay to further investigate

- how to extend its current monitor platform with performance and capacity planning modules
- request SoftChoice to add performance, throughput and bandwidth statistics to their Monthly VitalsReport
- investigate the SkyDrive/OneNote traffic that is current uploading data into the Cloud
- ensure that a fair use policy is in place and have be reflected in the policy rules of Vandelay's Internet facing gateways/firewalls.

¹ Gartner defines Shadow IT as IT devices, software and services outside the ownership or control of IT organizations.