TWELVEDOT

DESIGN.BUILD.SECURE

AGENDA

- Threats
- Standards and RFCs for Consideration
- Leveraging an ISMS
- Configuration Examples
- Considerations for the Future

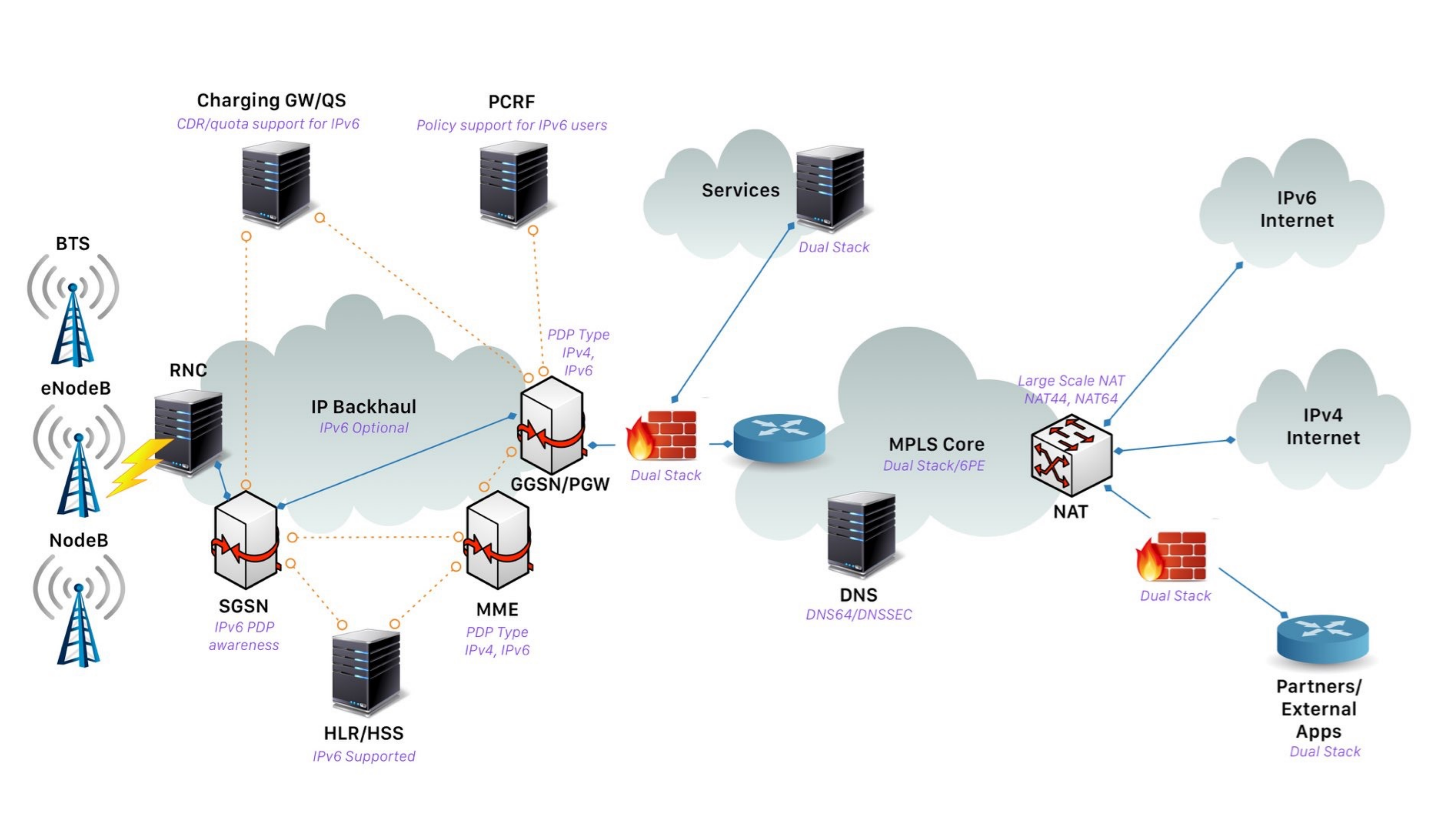
ABOUT US

- YOW CA based company
- Global customer base
- Focus on Mobile, Cloud and IoT Security
- Sister company focuses on HW/SW
- ISO standards are the basis for all our work
- Active in ISO/ITU standards development
- Core team of 7+ {global partnerships}

SECURITY IT NOT A TECHNOLOGY

I am not trying to scare you…..but educate you

IPV6 TOUCH POINTS



THREATS : OLDER

- Scanning of a /64 – thats crazy!
- Maturity of implementations
- Security product support for v6
- Complexity of attack surface vectors
- Confidence of staff for security issues to v6

THREATS : NEW

- NATs
- Identifying and Mitigating DoS/DDoS
- Stateful NAT not mature
- NATing $$$ with IPSec or TLS (session encryption) in terms of processing
- DNSSEC

THREATS : NEW

- Rogue DHCP Servers
- Targeting end points
- Leveraging Tunnels
- Fragmentation
    - Performed by hosts {never by routers}
    - Atomic frags have a Fragment Offset and M-bit = 0
    - Host fragments and opens itself to attack
- Many IPv4 vulns have been reimplemented in IPv6

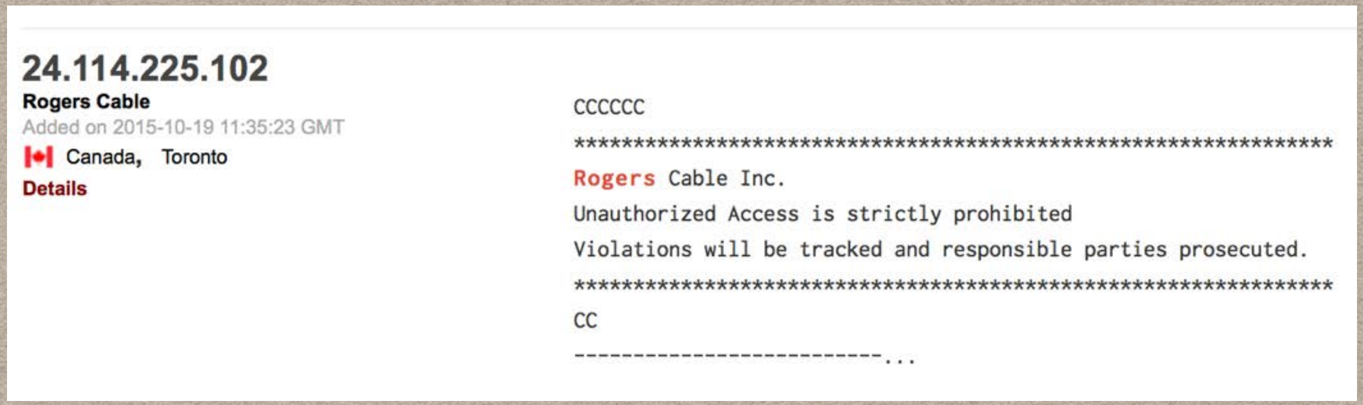
APPROACH

DEFENCE IN DEPTH

APPROACH TO AN ATTACK

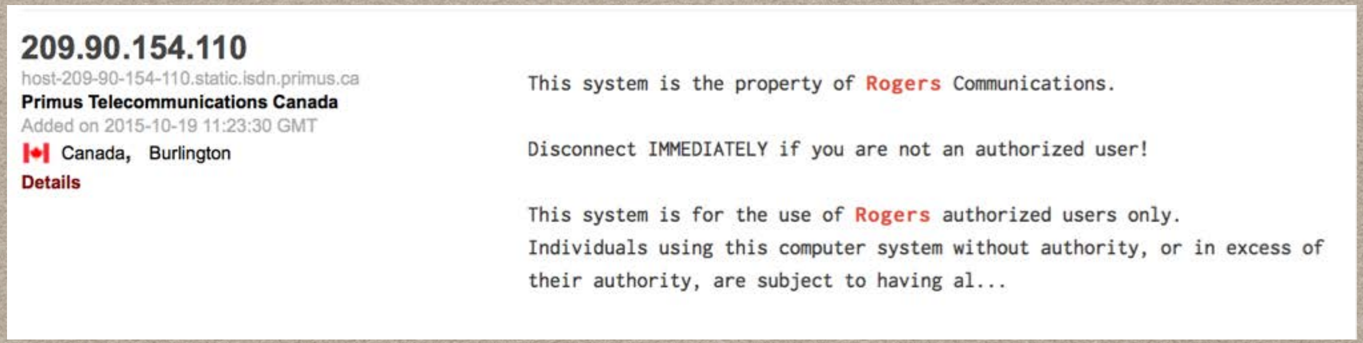
- Recon {active/passive}
- Vulnerability Scanning {if necessary}
- Exercising Options {atomic/aggressive}
- Test…..Fail……try again!
- Depending on the goal they never give up!
- Remember: Insider threat**

THREAT INTEL:1



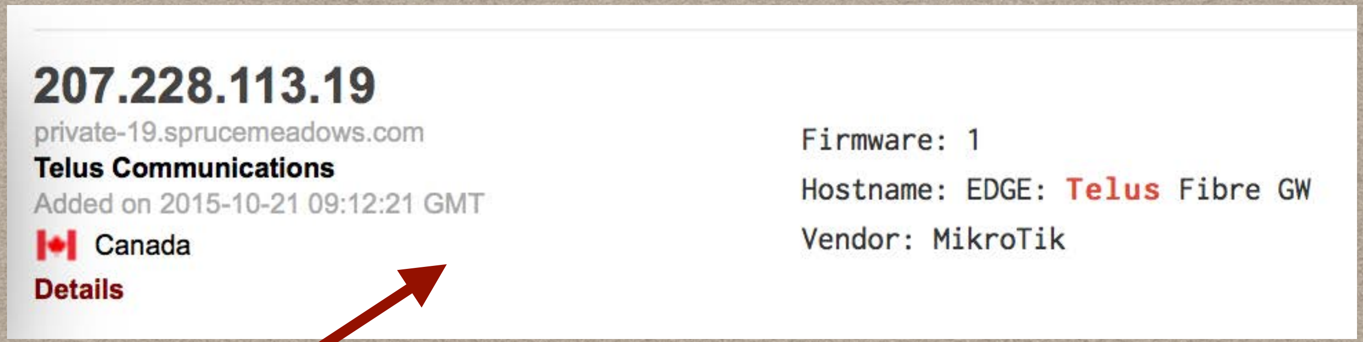
24.114.225.102
Rogers Cable
Added on 2015-10-19 11:35:23 GMT
Canada, Toronto
Details

```
CCCCCC
******************************************************************
Rogers Cable Inc.
Unauthorized Access is strictly prohibited
Violations will be tracked and responsible parties prosecuted.
******************************************************************
CC
---------------------------...
```



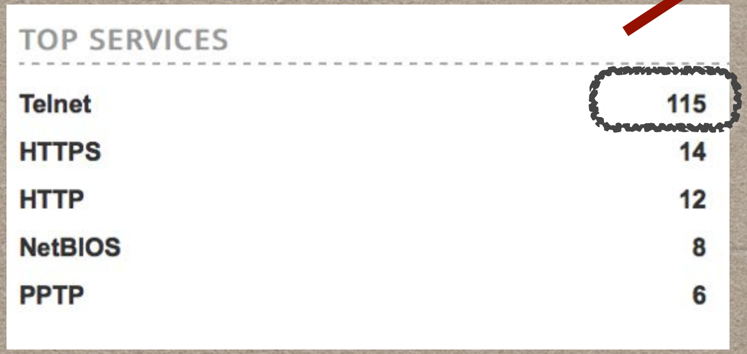
209.90.154.110
host-209-90-154-110.static.isdn.primus.ca
Primus Telecommunications Canada
Added on 2015-10-19 11:23:30 GMT
Canada, Burlington
Details

```
This system is the property of Rogers Communications.

Disconnect IMMEDIATELY if you are not an authorized user!

This system is for the use of Rogers authorized users only.
Individuals using this computer system without authority, or in excess of
their authority, are subject to having al...
```



207.228.113.19
private-19.sprucemeadows.com
Telus Communications
Added on 2015-10-21 09:12:21 GMT
Canada
Details

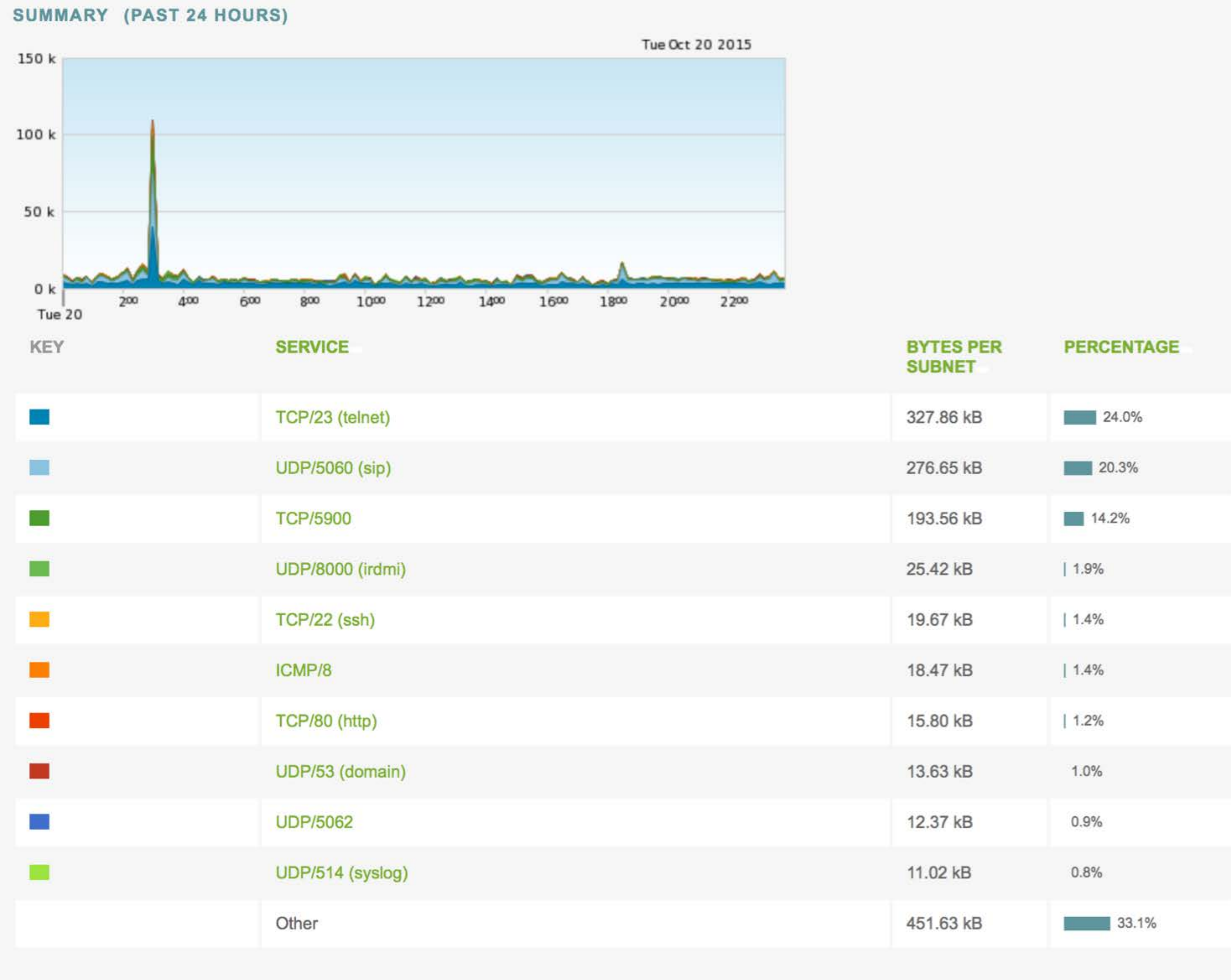
```
Firmware: 1
Hostname: EDGE: Telus Fibre GW
Vendor: MikroTik
```



TOP SERVICES	
Telnet	115
HTTPS	14
HTTP	12
NetBIOS	8
PPTP	6

Source: shodan.io

THREAT INTEL:2

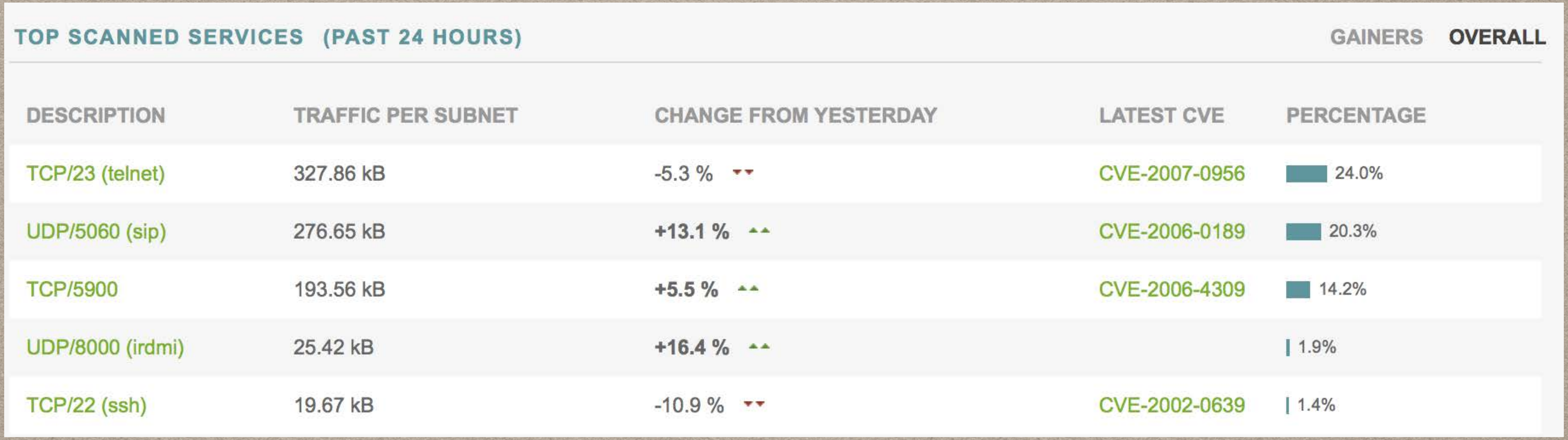


SUMMARY (PAST 24 HOURS)

KEY	SERVICE	BYTES PER SUBNET	PERCENTAGE
🟦	TCP/23 (telnet)	327.86 kB	24.0%
🟦	UDP/5060 (sip)	276.65 kB	20.3%
🟩	TCP/5900	193.56 kB	14.2%
🟩	UDP/8000 (irdmi)	25.42 kB	1.9%
🟨	TCP/22 (ssh)	19.67 kB	1.4%
🟧	ICMP/8	18.47 kB	1.4%
🟥	TCP/80 (http)	15.80 kB	1.2%
🟥	UDP/53 (domain)	13.63 kB	1.0%
🟦	UDP/5062	12.37 kB	0.9%
🟩	UDP/514 (syslog)	11.02 kB	0.8%
	Other	451.63 kB	33.1%

Source: atlas.arbournetworks.com

THREAT INTEL:3



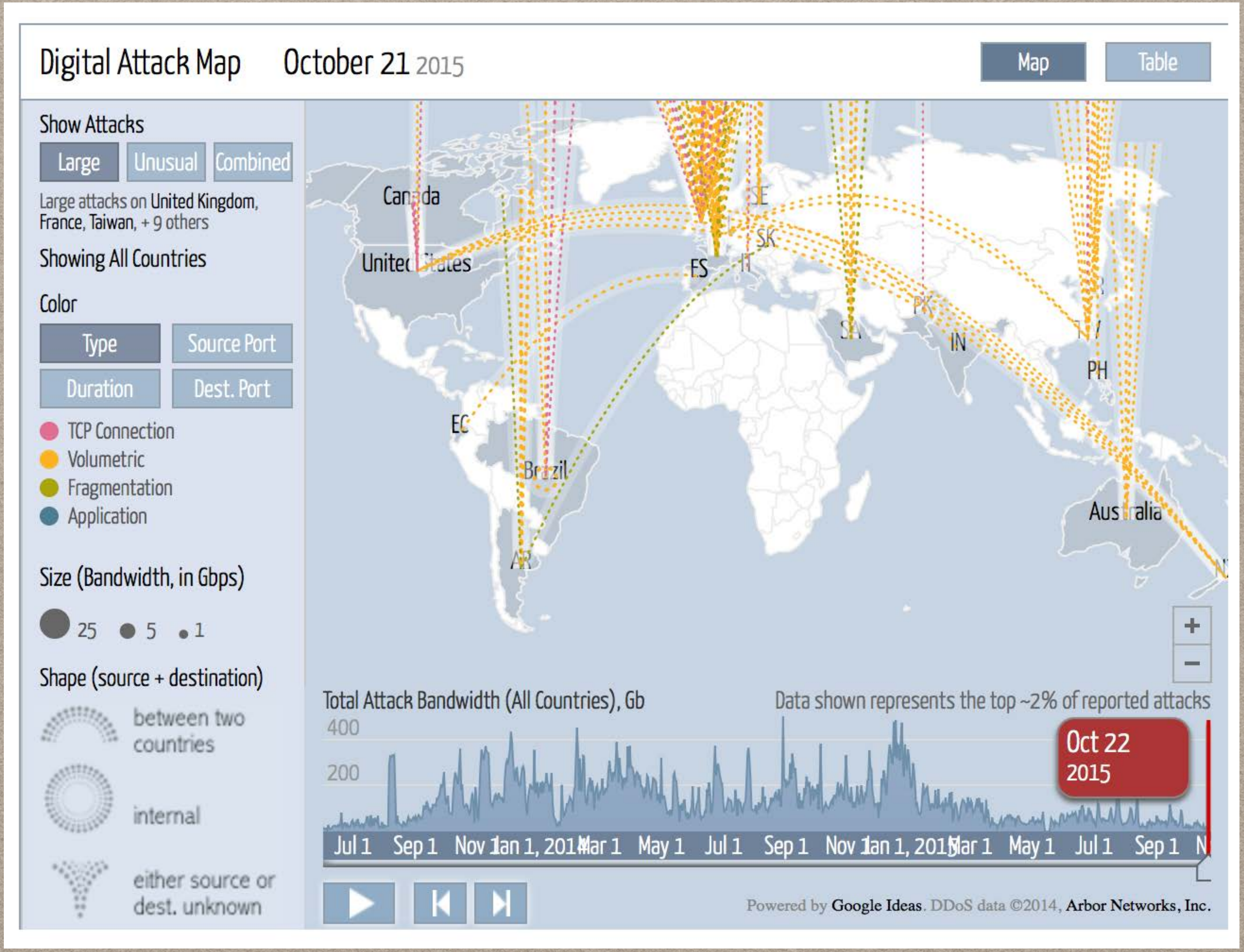
TOP SCANNED SERVICES (PAST 24 HOURS)

DESCRIPTION	TRAFFIC PER SUBNET	CHANGE FROM YESTERDAY	LATEST CVE	PERCENTAGE
TCP/23 (telnet)	327.86 kB	-5.3 % ▼▼	CVE-2007-0956	24.0%
UDP/5060 (sip)	276.65 kB	**+13.1 %** ▲▲	CVE-2006-0189	20.3%
TCP/5900	193.56 kB	**+5.5 %** ▲▲	CVE-2006-4309	14.2%
UDP/8000 (irdmi)	25.42 kB	**+16.4 %** ▲▲		1.9%
TCP/22 (ssh)	19.67 kB	-10.9 % ▼▼	CVE-2002-0639	1.4%

http://map.norsecorp.com

Source: atlas.arbournetworks.com

THREAT INTEL:4



Large attacks on United Kingdom, France, Taiwan, + 9 others

Data shown represents the top ~2% of reported attacks

Powered by Google Ideas. DDoS data ©2014, Arbor Networks, Inc.

http://map.norsecorp.com

Source: atlas.arbournetworks.com

APPROACH TO SECURITY

- Need to have “culture” of security
- Good policies & procedures
- Risk Management
- Testing and Evaluation
- Don’t downplay the insider threat
- Threat Profiling

STANDARDS : ISO

- Need to implement an ISMS {ISO27001/2:2013}
  - Provides an overall all stronger security posture for the company and operations
  - Drives security risk management as a business function
  - Audit-able and provides traceability
  - Defines security requirements for partners, vendors, and App providers

LEVERAGING A ISMS

- Why?
  - Ensures a consistent approach to cyber security
  - High level of security assurance
  - Aligns to corporate goals
- Target alignment to ISO27K to start
- Governance of Ops, network vendors, and App partners

LEVERAGING A ISMS: CONCEPTS

- Risk Identification and Mitigation
- HR Practices {including training and awareness}
- Incident Handling
- Operational (NOC)

Building on what you have and making it more formalized as a business practice

STANDARDS : IETF

- RFC 7123 Security Implications of IPv6 on IPv4 Networks
- RFC 7527 Enhanced Duplicate Address Detection
- RFC 3704 Ingress Filtering for Multihomed Networks
- RFC 6494 Certificate Profile and Certificate Management for Secure Neighbour Discovery
- RFC 6946 Processing of IPv6 "Atomic" Fragments
- RFC 4942 IPv6 Transition/Co-existence Security Considerations
- Info: Possible Attack on Cryptographically Generated Addresses (CGA)
- Info: Recommendations for Local Security Deployments

ADDRESSING SECURITY:1

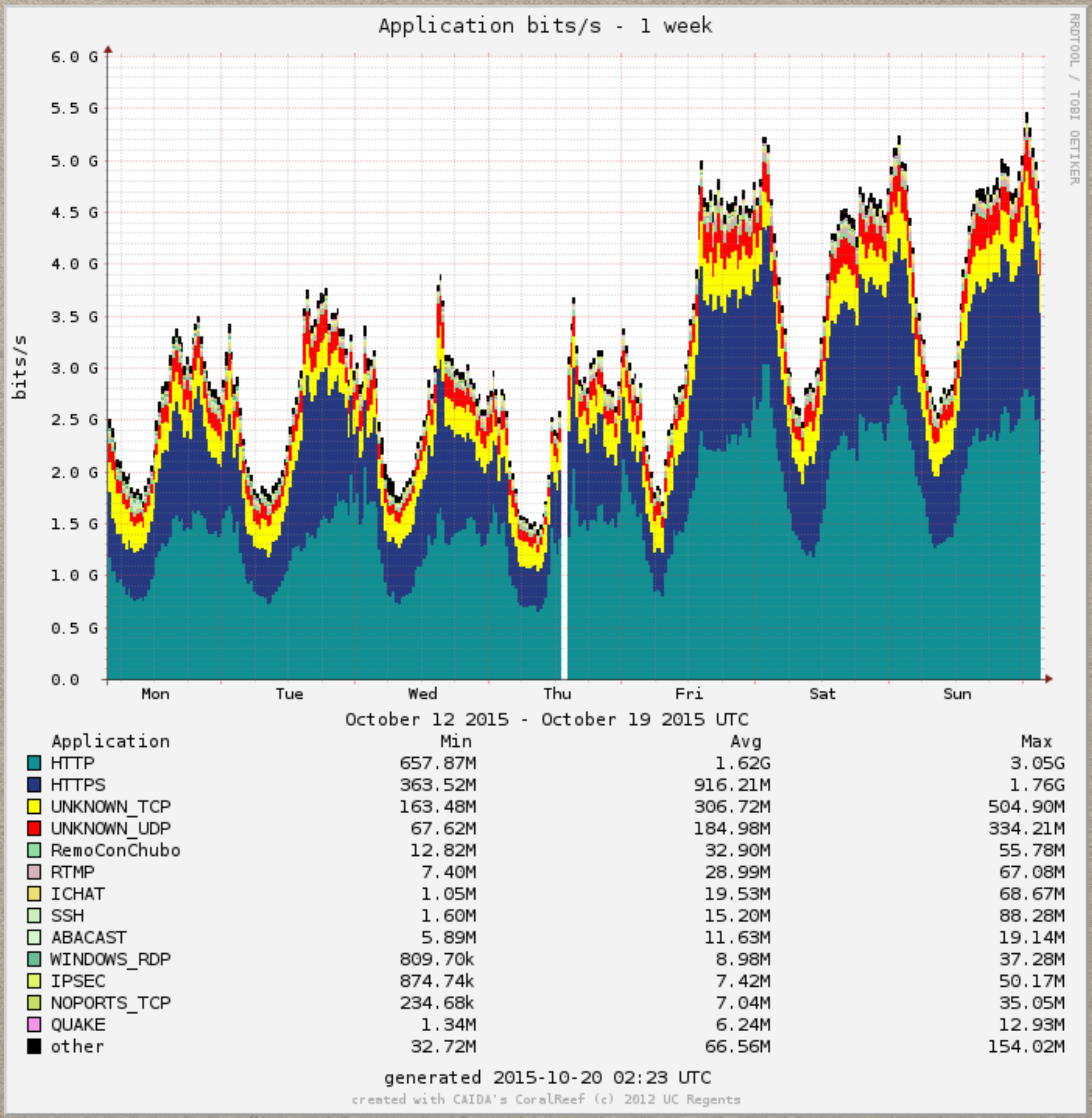
- Advertisement Guard (RA-Guard) for attacks based on Stateless Address Autoconfiguration (SLAAC)
  - Filter Router Advertisements on L2 before they reach the target
  - Define SRC, INT, Auth SRC
  - Runs in stateful and stateless mode
  - Depends router L2 ability to detect RA msg
  - Extension Headers {i.e. Fragmentation} see RFC 7113 for guidance
- DHCPv6-Shield [SHIELD] to mitigate DHCPv6-based attacks
  - Blocks malicious DHCPv6-server packets at layer-2
  - Complements RA-Guard

ADDRESSING SECURITY:2

- Tunnelling
  - Use dual stack as migration path
  - Use static vs. dynamic tunnelling {6to4}
  - Use outbound filtering on FW to allow only authorized tunneling endpoints
  - Monitor via IPS and NetFlow
- NAT
  - Document procedure for last-hop traceback
  - 20-bit Flow Label field in the IPv6 header

ADDRESSING SECURITY:3

- IPSec
  - Not a silver bullet
  - < 1% of Internet Traffic
- IPSec can be deployed in three architectures:
  - gateway to gateway
  - node to node
  - node to gateway
- Remember: Encrypted attack traffic is still attack traffic



October 12 2015 - October 19 2015 UTC

	Application	Min	Avg	Max
🟦	HTTP	657.87M	1.62G	3.05G
🟦	HTTPS	363.52M	916.21M	1.76G
🟨	UNKNOWN_TCP	163.48M	306.72M	504.90M
🟥	UNKNOWN_UDP	67.62M	184.98M	334.21M
🟩	RemoConChubo	12.82M	32.90M	55.78M
▨	RTMP	7.40M	28.99M	67.08M
🟨	ICHAT	1.05M	19.53M	68.67M
🟩	SSH	1.60M	15.20M	88.28M
▨	ABACAST	5.89M	11.63M	19.14M
🟩	WINDOWS_RDP	809.70k	8.98M	37.28M
🟨	IPSEC	874.74k	7.42M	50.17M
🟩	NOPORTS_TCP	234.68k	7.04M	35.05M
🟪	QUAKE	1.34M	6.24M	12.93M
■	other	32.72M	66.56M	154.02M

generated 2015-10-20 02:23 UTC

created with CAIDA's CoralReef (c) 2012 UC Regents

ADDRESSING SECURITY:4

- Dual stack
  - Implement RFC 2827 filtering
- Firewall
  - Determine extension headers permitted through access control devices
  - Determine required ICMPv6 msg required
  - Filter unneeded services at FW
  - Treat fragments like regular packets {don’t queue}
  - Block all IPv6 destined to IPv4 only networks

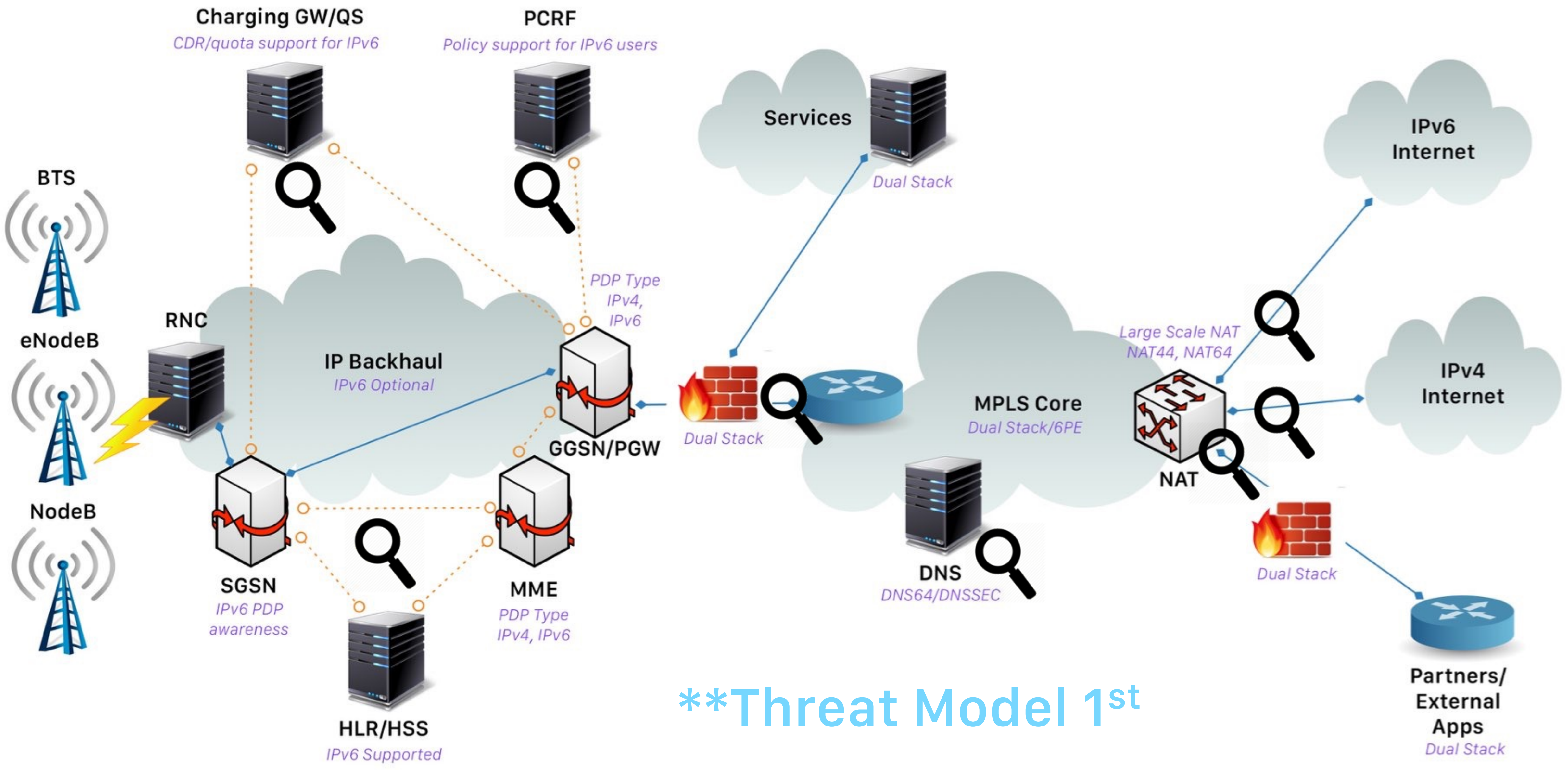
ADDRESSING SECURITY:5

- 1st Hop Strategy
  - Using ICMP Snooping, DHCPv6 Guard, and IPv6 Destination Guard {ND to address resolution only for those addresses that are known to be active on the link}
- Other
  - Use non-obvious addresses for critical systems {and monitor}
  - Deny IPv6 frags dst to internetworking devices {when possible}
  - Use IPSec to provide auth and confidentiality to service assets
  - Keep monitoring for zero days on vendor gear!

ADDRESSING SECURITY:6

- Evaluating Security Technology
  - Don’t buy the marketing ask for pilots and demo the product for 60-90 days in your lab
  - Use packet generators and testing tools
  - Create and maintain security test sets/requirements
  - Setup a lab to train staff
- Don’t be afraid to give you vendor candid feedback

MONITORING



**Threat Model 1st

ON GOING ACTIVITIES

- Ensure your scanning and testing for weaknesses
  - THC's IPv6 attack suite
  - SI6 Networks IPv6 toolkit
- Enforcing security controls for both v4/v6 traffic
- Leverage your ISMS
- Create a security guide for deployment of new devices

FINAL THOUGHTS

- Create a culture of security in your organization
- Apps will “always” be a target
- IPv6 security still need lots of work but we are making progress
- Need to approach each layer as separate and deal with controls differently as well
- Eliminate the dependancy on NAT ASAP
- DoS, L7 and rogue devices will still plague operators

OPEN DISCUSSION AND QUESTIONS

THANK-YOU FOR YOUR TIME TODAY

Faud Khan

faud.khan@twelvedot.com

www.twelvedot.com

+1 613 447 3393