Network Barometer Report 2012

Results summary

About the Network Barometer Report

Research Sample

Security Vulnerabilities

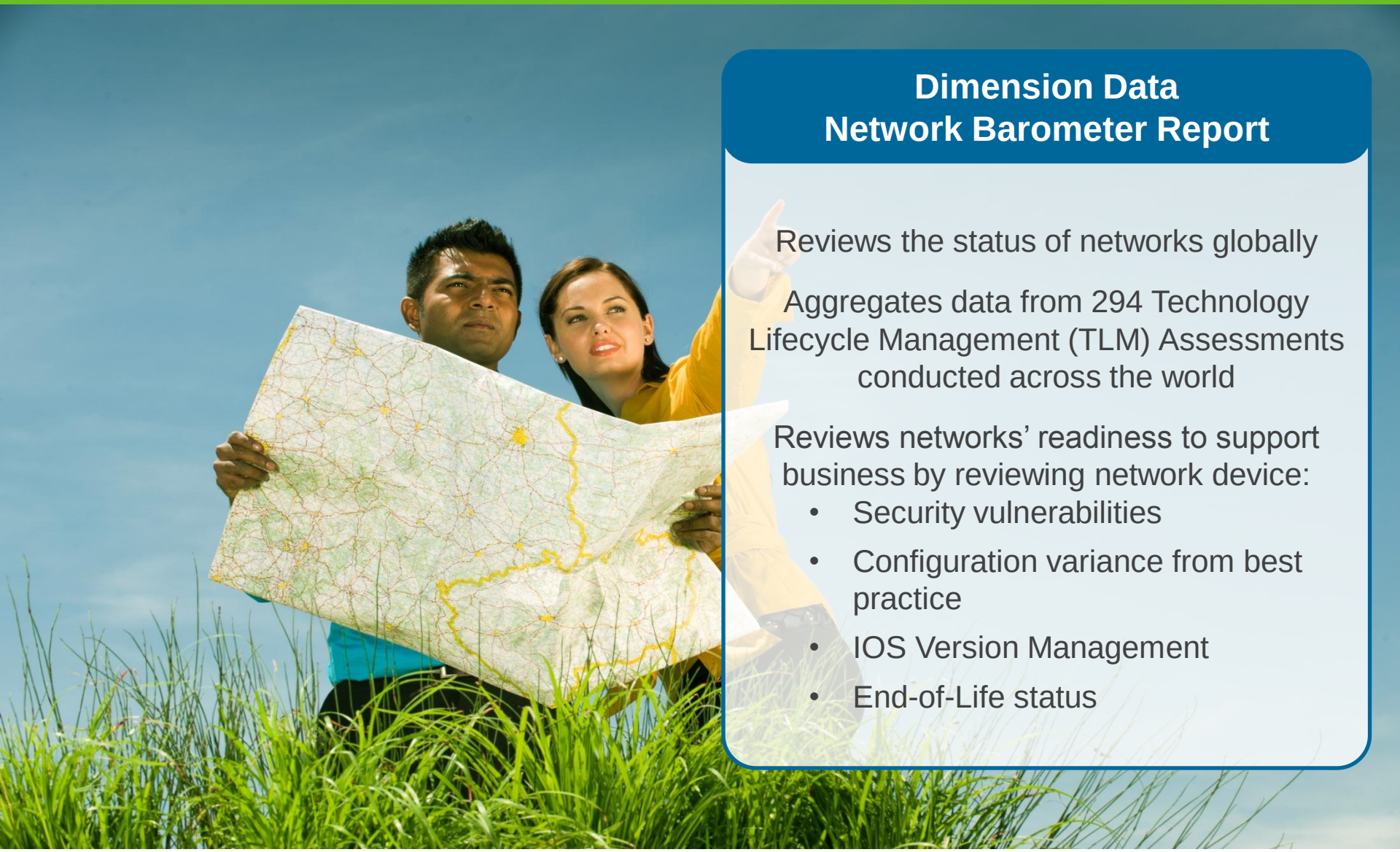
Configuration Issues

IOS Version Management

Technology Lifecycle Status

Architecture vs. Obsolescence

The Network Barometer Report looks at how ready networks are to support business



Dimension Data Network Barometer Report

Reviews the status of networks globally

Aggregates data from 294 Technology Lifecycle Management (TLM) Assessments conducted across the world

Reviews networks' readiness to support business by reviewing network device:

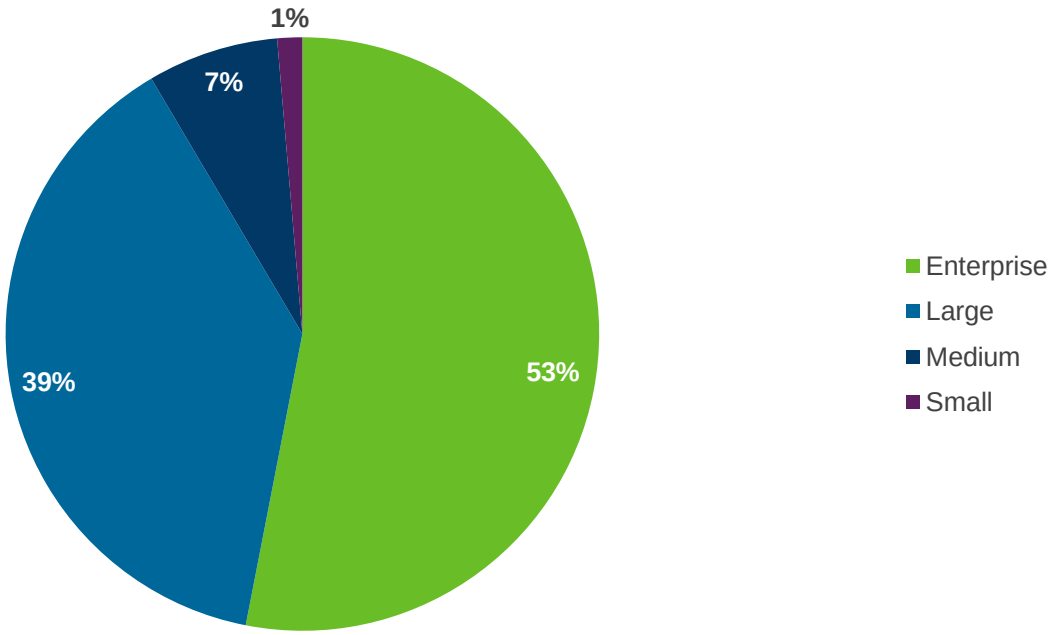
- Security vulnerabilities
- Configuration variance from best practice
- IOS Version Management
- End-of-Life status

2012 Highlights

- 75% of network devices are carrying at least one known security vulnerability, in line with the 73% in 2011.
- A single vulnerability was responsible for this high PSIRT penetration. PSIRT 10944, identified by Cisco in September 2009, was found in 47% of all the devices analysed during 2011
- While the number of configuration errors per device increased from 29 to 43, security related configuration errors such as AAA Authentication continue to dominate
- The percentage of devices that entered the obsolescence phase increased from 38% to 45%
- Of those devices, the percentage that were End-of-Sale jumped from 4.2% in 2011 to 70% in 2012. The percentage of devices that were either Eo SW maintenance EoCR dropped a similarly dramatic amount from 86.2% to 20.8%.
- A third of all Wireless access points discovered during the calendar year 2011 were 802.11n-capable. This is nearly triple the 12% 802n penetration from last year. This adoption will also drive refresh in the underlying routing and switching infrastructure

The sample size is heavily weighted towards enterprise and large sized organisations.

Sample distribution by organisation size

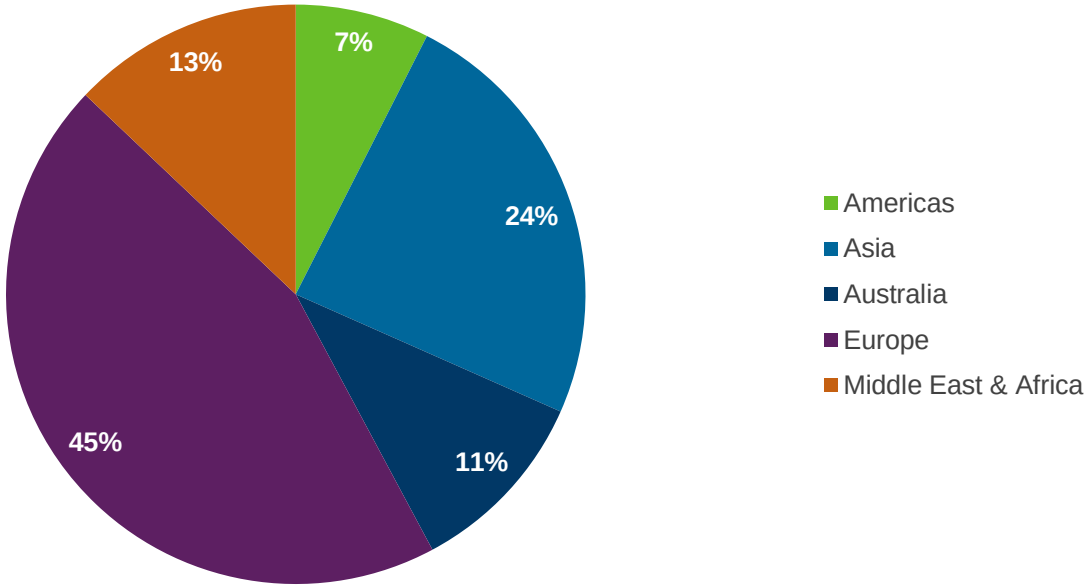


- Small – fewer than 100 users
- Medium – greater than 100, but fewer than 500 users
- Large – greater than 500, but fewer than 2500 users
- Enterprise – greater than 2500 users

The sample is broadly representative of networks around the world.

Sample distribution by geography

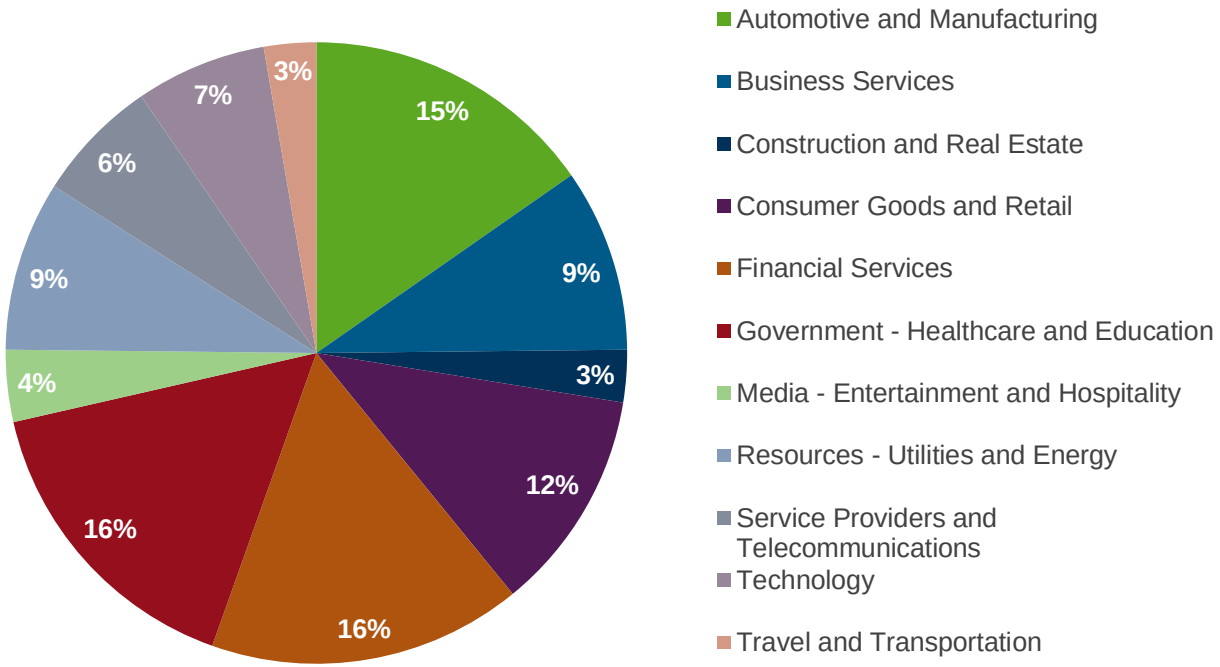
(see the Appendix for a Country Breakdown)



- Europe includes Belgium, Czech Republic, France, Germany, Italy, Luxembourg, the Netherlands, Spain, Switzerland and the United Kingdom
- Americas include Canada, USA, Brazil and Mexico
- Middle East and Africa is primarily South Africa
- Asia includes China, Hong Kong, India, Indonesia, Japan, Malaysia, New Zealand, Philippines, Singapore and Vietnam

Representation across industries is broadly reflective of the adoption of IT and associated spend across vertical sectors.

Sample distribution by vertical industry sector



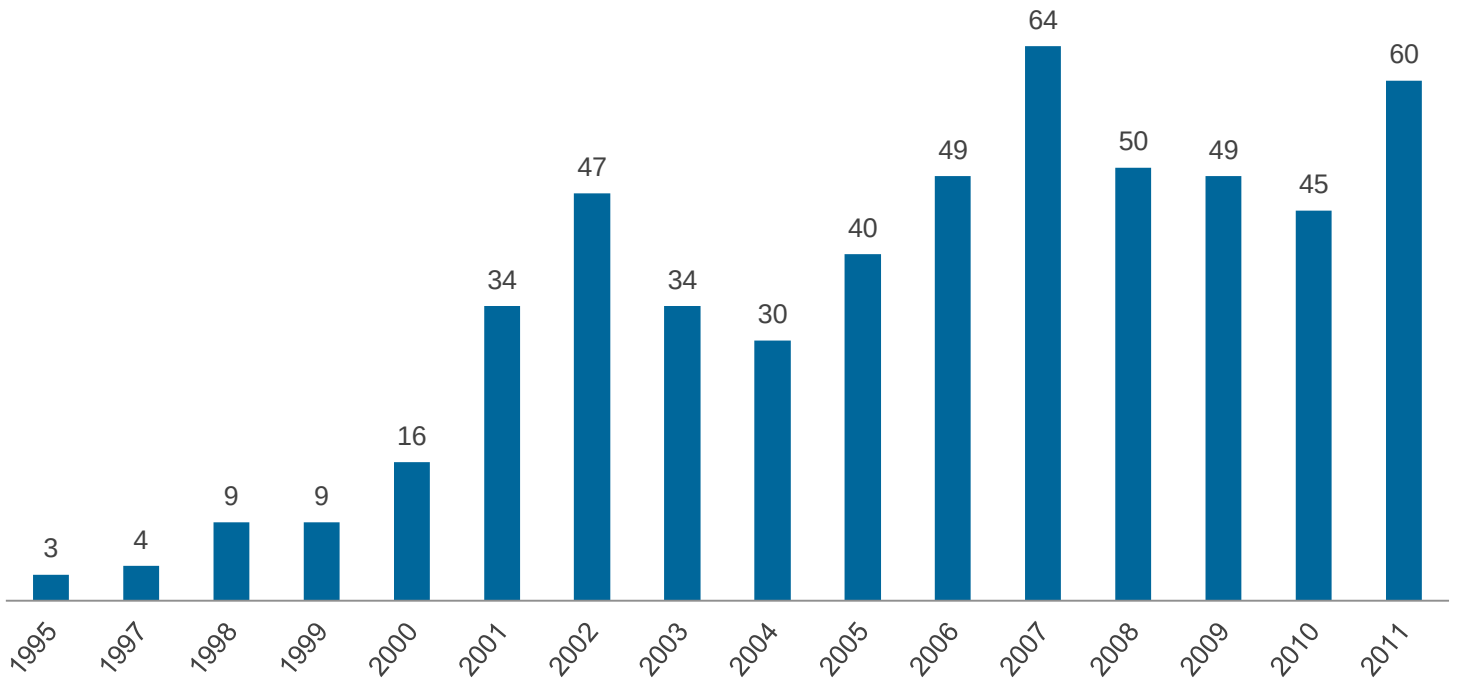
- Financial Services and Government , Healthcare and Education make up one-third of the sample. Therefore results will be particularly applicable to these sectors.
- Outside of the two verticals above, the remaining assessments were reasonably spread across the remaining vertical industries.

Security Vulnerabilities

In the context of the Report, vulnerabilities relate to existing known defects in the software, for which the manufacturer has a recommendation for remediation.

The number of new vulnerabilities identified by Cisco each year is on the decline.

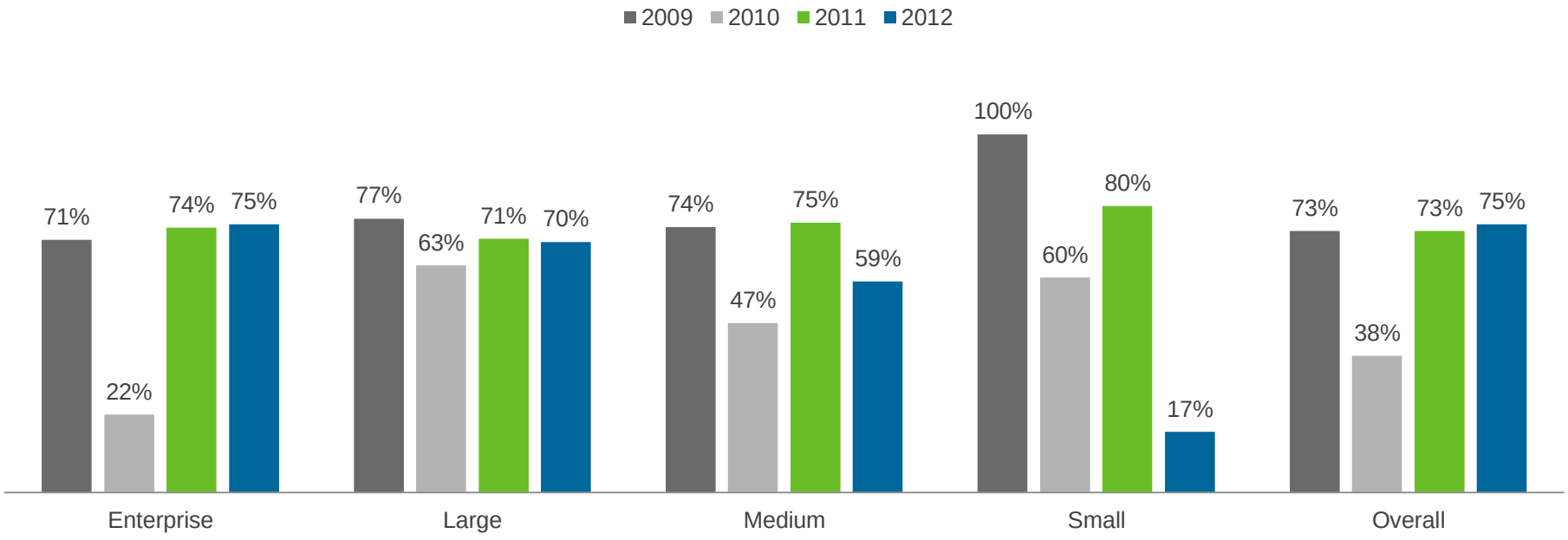
Security vulnerabilities identified per year



- After peaking at 64 new PSIRTS in 2007, the announcements had tapered off in the 45 to 50 range for the past three years, before spiking again to 60 in in 2011

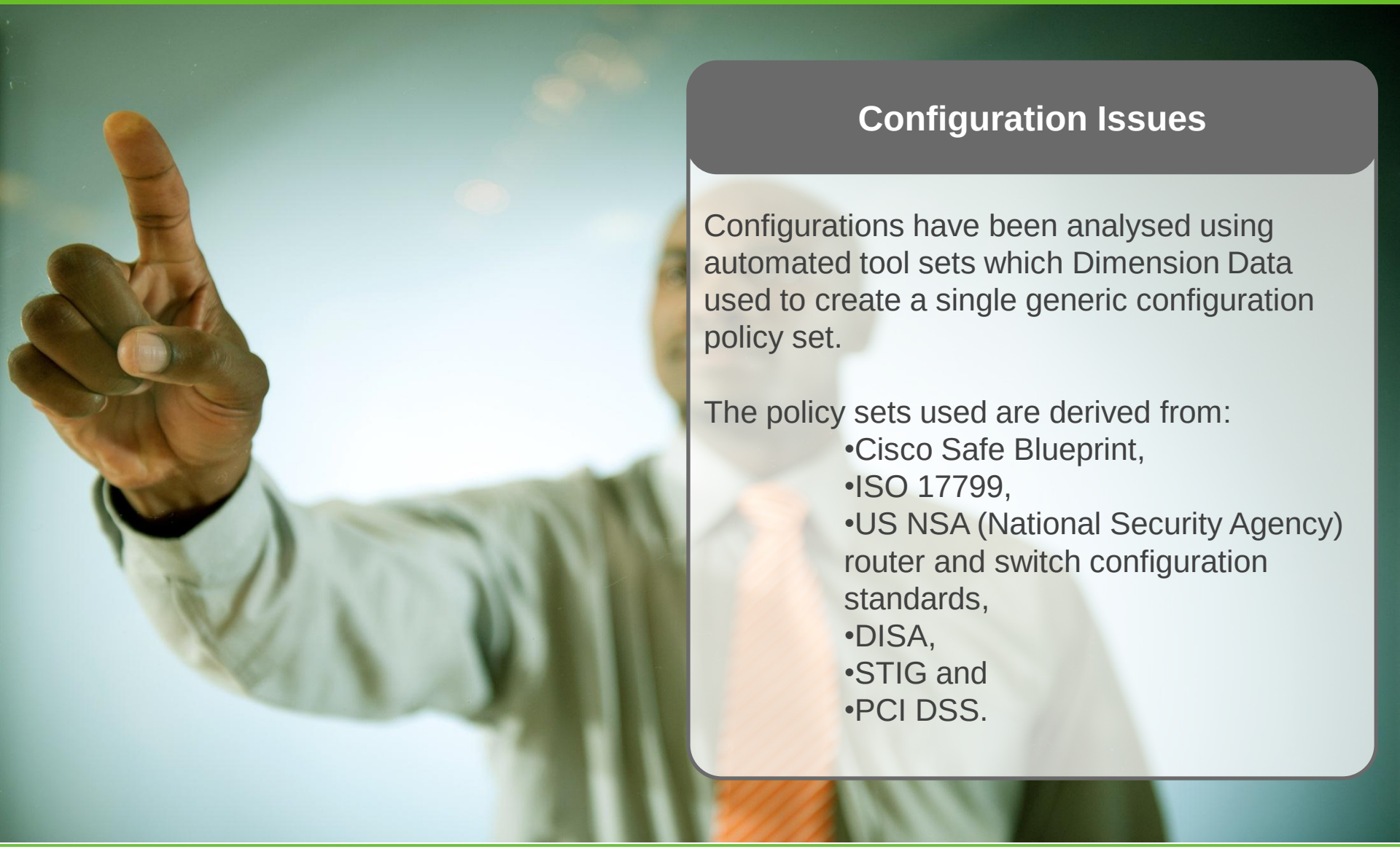
Of all of the devices analysed, 75% are carrying at least one known security vulnerability.

Average % of devices with security vulnerabilities by organisation size



- 75% of all devices carry at least one known security vulnerability. This figure is statistically consistent with the 73% figure of the previous year.
- A single vulnerability was responsible for this high PSIRT penetration. PSIRT 10944, identified by Cisco in September 2009, was found in 47% of all the devices analysed during 2011

Configuration Issues



Configuration Issues

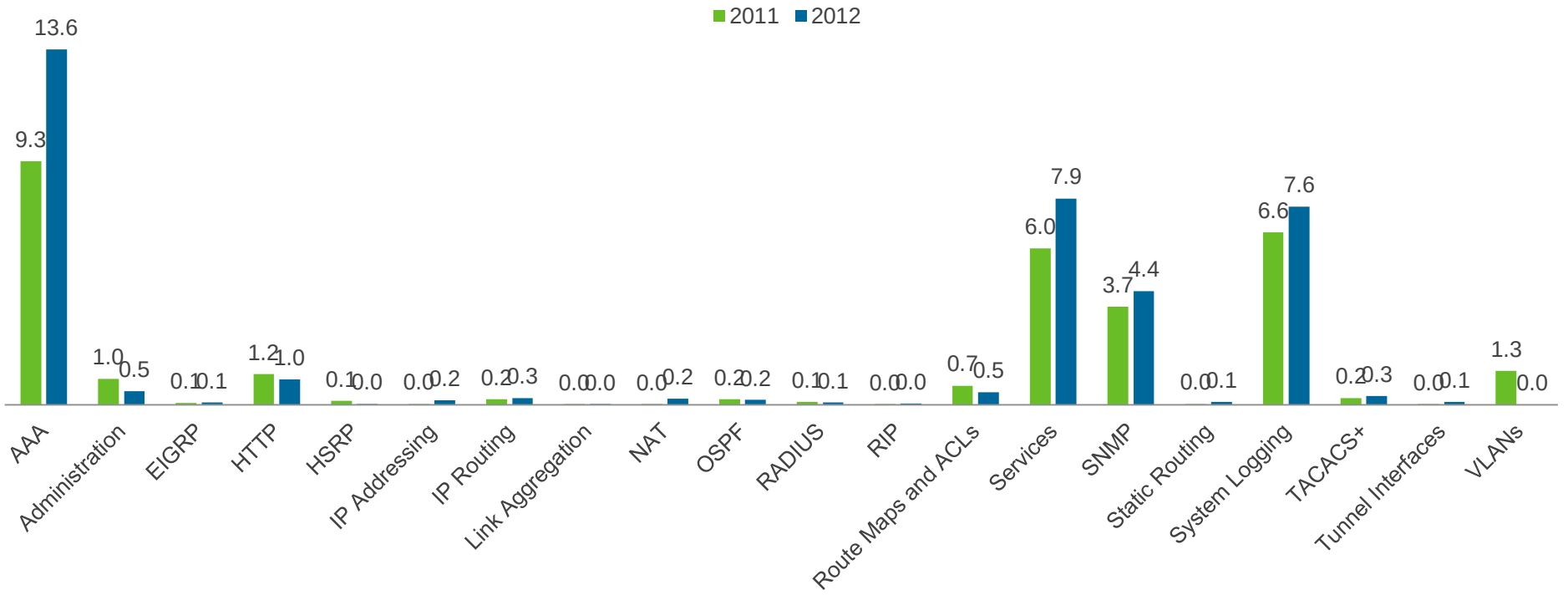
Configurations have been analysed using automated tool sets which Dimension Data used to create a single generic configuration policy set.

The policy sets used are derived from:

- Cisco Safe Blueprint,
- ISO 17799,
- US NSA (National Security Agency) router and switch configuration standards,
- DISA,
- STIG and
- PCI DSS.

Overall number of configuration errors has increased and AAA errors continue to dominate.

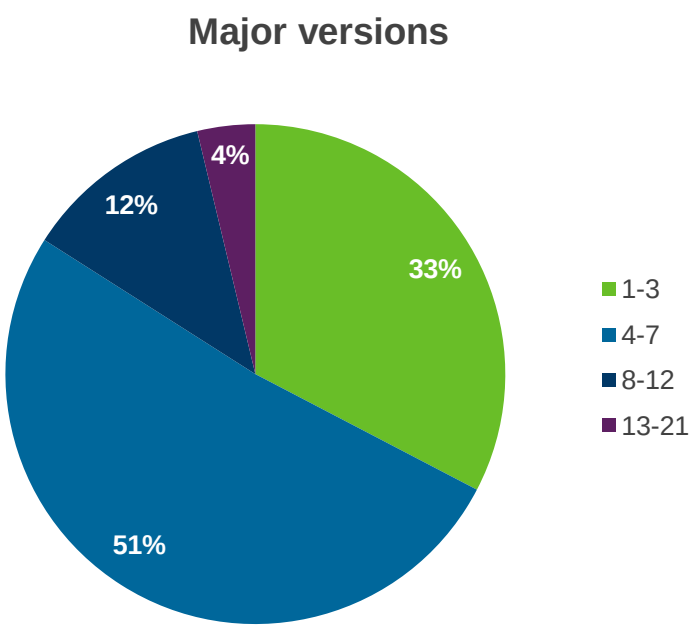
Average number of policy violations per device per configuration category

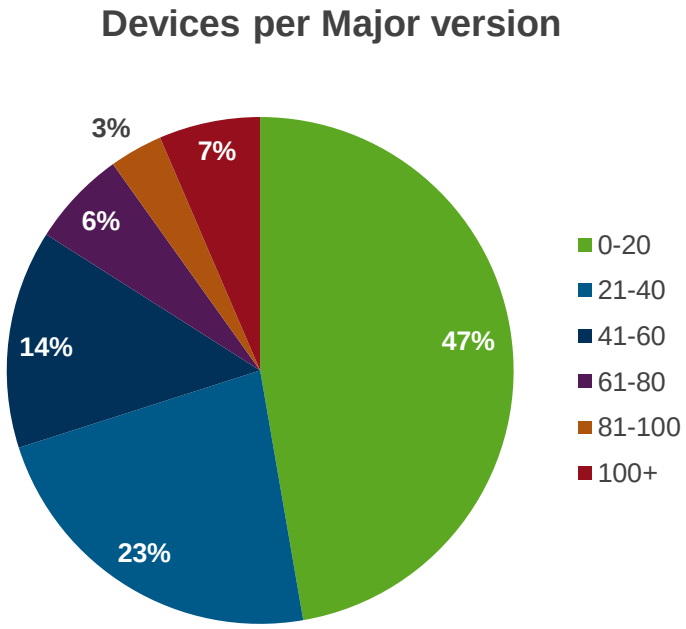


- The total number of configuration violations per device increased from 29 to 43, which is a regression to 2009 levels
- AAA Authentication errors in particular jumped from 9.3 per device in in the previous year to 13.6 this year and continue to be the most frequently occurring policy violation.

Managing the number of unique versions of IOS can be an operational challenge

Number of assessments categorised by count of major versions of IOS





- The data shows an average of 5.1 major versions of IOS and 20.3 unique versions of IOS were discovered per assessment.
- In the most extreme cases, clients had as many as 21 major versions and 153 minor versions of IOS.
- Comparing data from last year's Network Barometer report, we note that there hasn't been a substantial change in the number of unique versions of IOS

Technology Lifecycle Status

Technology Lifecycles

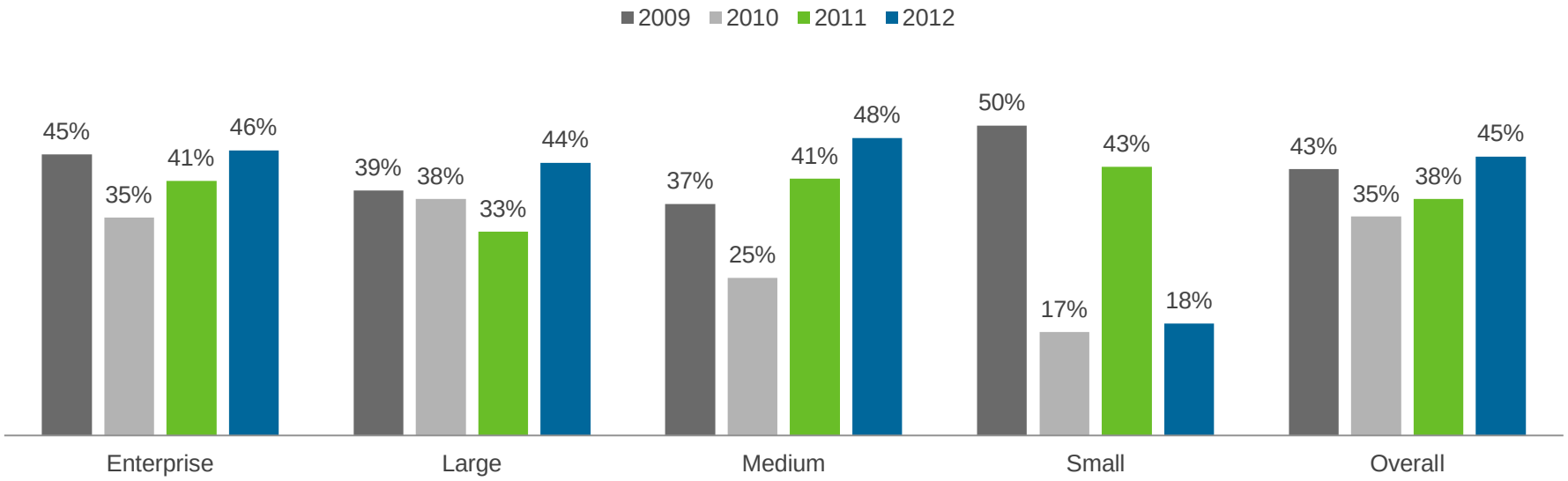
Vendors have standardised end-of-life milestones through which they progress their products
towards obsolescence.

Technology at EoS (end-of-sale) status is regarded as an aging asset and will be increasingly unsupportable and exposed to risk as it progresses towards LDoS (last-day-of-support).

By EoSWM (end-of-software-maintenance), any new bugs found on the software will no longer be patched opening the organisation up to availability and mean time to repair (MTTR) risks

The percentage of client networks that have entered the obsolescence cycle has increased steadily.

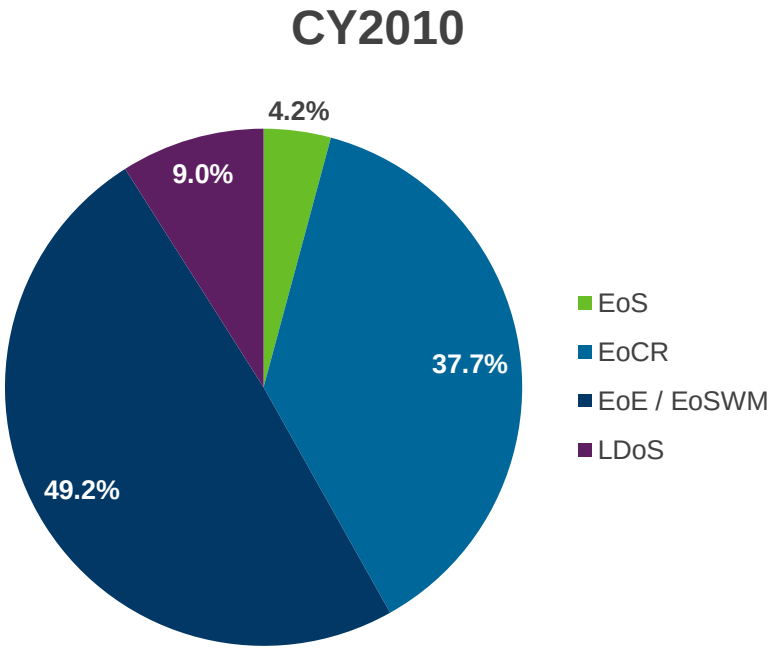
Average % of devices beyond EoS by organisation size

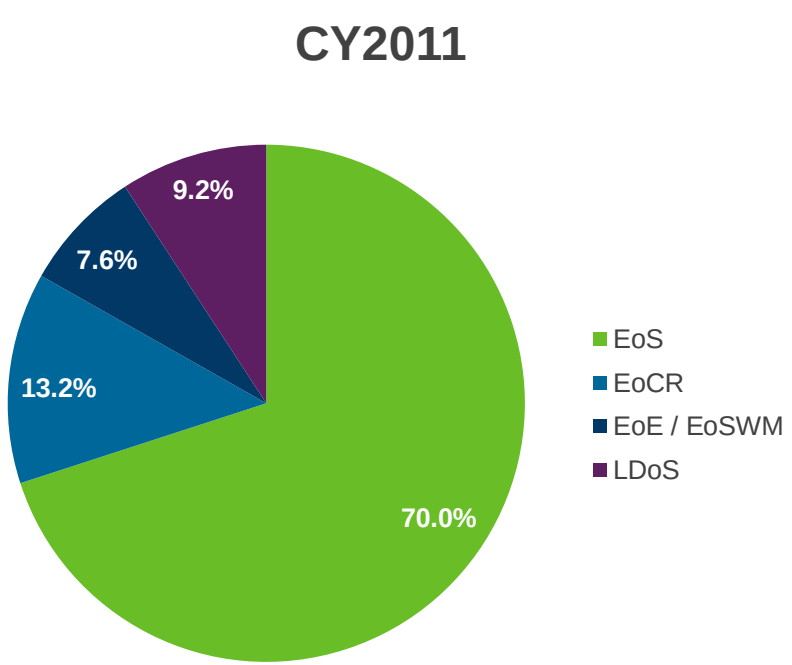


- On average, 40% of all devices have been past EoS for the past four years. That said, there have been small year–on-year increases over the past three years – 3% from 2010 to 2011 and 7% from 2011 to 2012.
- This suggests a trend of increasing obsolescence in network estates.

Dramatic change in the breakdown of devices by their lifecycle category

Milestone distribution of devices by end of life cycle stage



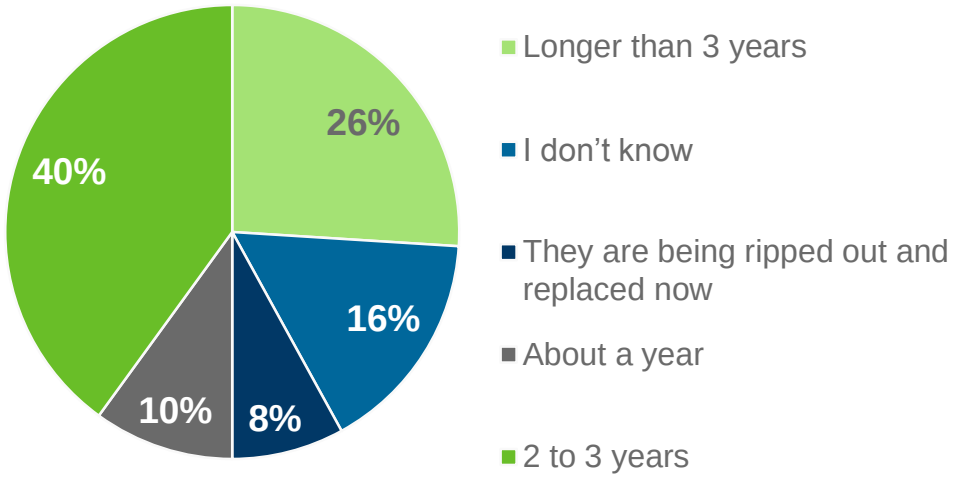


- The percentage of devices that were simply EoS (the earliest lifecycle milestone and therefore the least risky) jumped from 4.2% in 2011 to 70% in 2012.
- The percentage of devices that were either EoE/EoSWM or EoCR (which carry medium to high level risk) dropped a similarly dramatic amount from 86.2% to 20.8%.
- The percentage of devices that were LDoS (the final stage of obsolescence and the highest level of risk) remained unchanged at 9%.

Enterprise Mobility and BYOD drives 802.11n refresh

Maintenance Timeframe for 802.11a/b/g networks

Approximately how long do you estimate you will maintain your 802.11 a/b/g network



Information Week Analytics 2011 Wireless LAN Survey, Sept 2010 (Base: 242 respondents)

Discovered AP's in TLM assessment base that support 802.11n

2010

12%

2011

33%

- A third of all access points discovered during the calendar year 2011 were 802.11n-capable. This is nearly triple the 12% 802n penetration from last year. Given the market trend towards increased mobility demands, there it is likely that 802.11n access point penetration will be greater than 50% next year.
- Continued 802.11n adoption will continue to drive refresh in core networks- Only 32% of all access switches discovered during the calendar year 2011 supported gigabit Ethernet while another 48% supported PoE and only 18% supported PoE+

For the full version of the Network Barometer Report 2012 go to

www.dimensiondata.com/networkbarometer