



# Switch Testing Made Difficult

---

David Newman  
Network Test



# Network World switch test

---

- Test published 24 March 2008
  - <http://www.networkworld.com/reviews/2008/032408-switch-test.html>
- Access switches (48 x GE, 2 x 10GE)
  - Alcatel-Lucent OmniSwitch 6850
  - Cisco Catalyst 3750E
  - D-Link DGS 3650
  - Dell PowerConnect 6248P
  - Extreme Summit X450a-48t
  - Foundry FastIron X448
  - HP ProCurve 3500yl

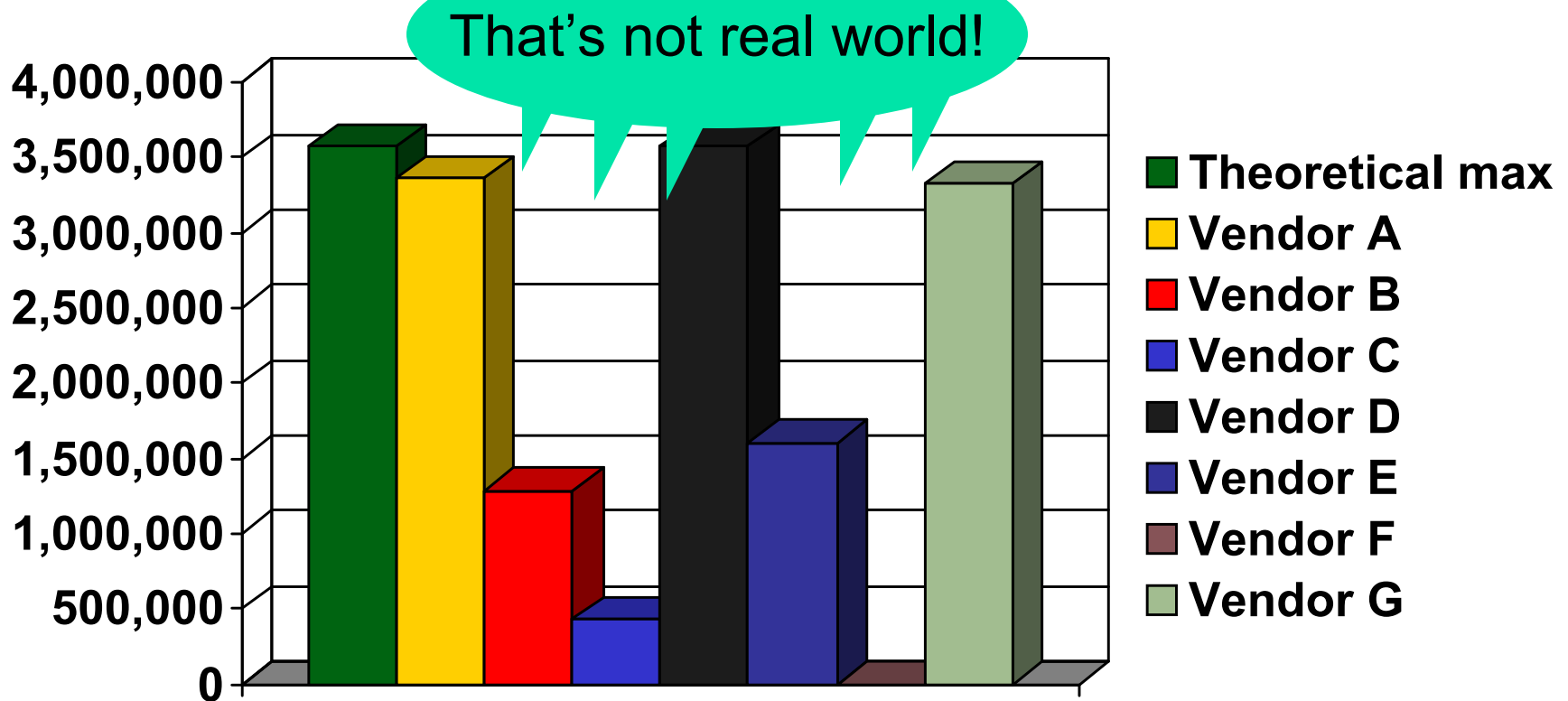


# Switch testing: The good old days?

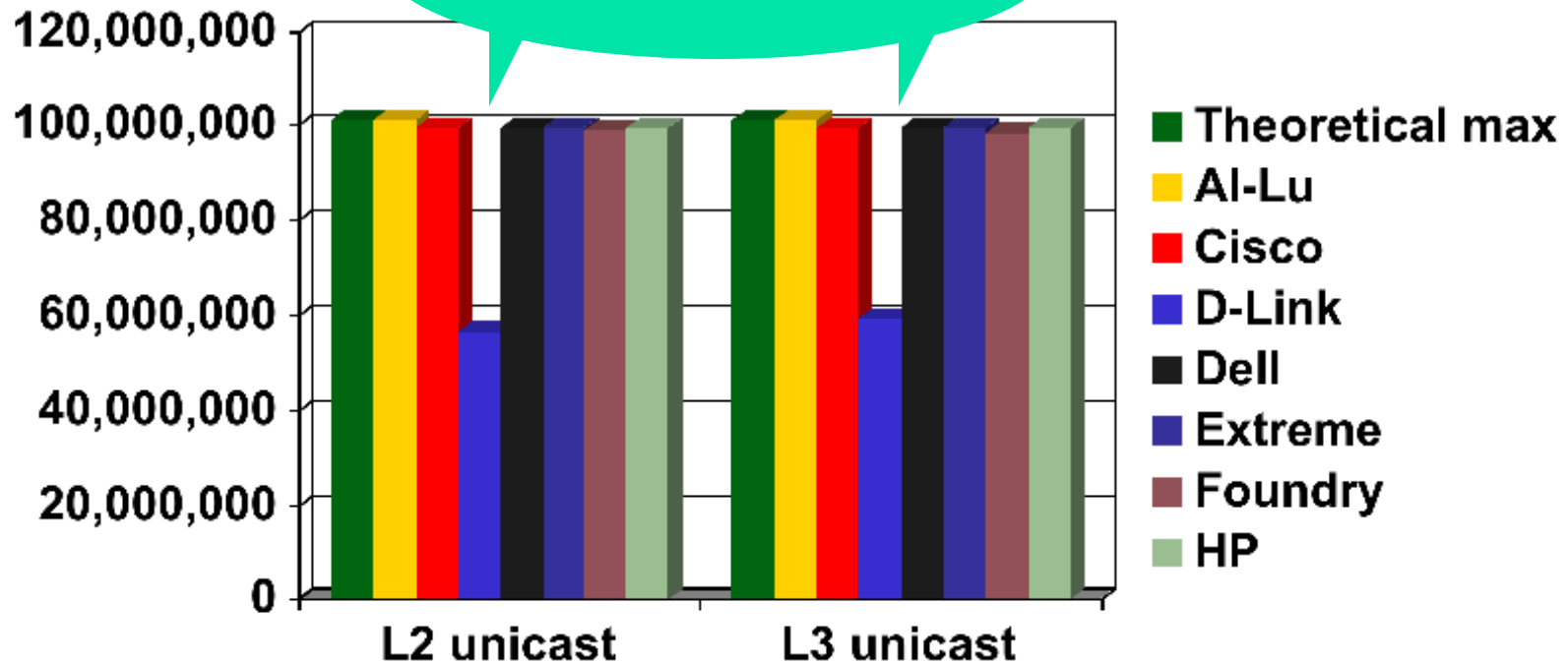
---

- It was all about performance
  - L2 throughput
  - L2 latency
  - L2 address cache capacity (maybe)
  - Everything in 2 RFCs: 2285, 2889
- That's all, folks

# Throughput testing, old school



# Throughput testing today





# What changed?

---

- 1999-2001: Broadcom, Marvell, others introduce “merchant silicon”
  - Switches now cheap, easy to build
- 2001-today: Asia Inc. commoditizes
  - At least 60-70 domestic-only Ethernet manufacturers in China today



# Switch testing today

---

- L2 unicast performance
  - (throughput, latency, jitter)
- L3 unicast performance
- L2 multicast group capacity
- L2 multicast performance
- L3 multicast performance
- 802.1X/network admission control
- Storm control
- Power consumption
- IPv4/IPv6 manageability
- Usability
- Management



## Switch testing today (cont'd)

---

- RFC 1242/2544
  - RFC 2285/2889
  - RFC 2412/3918
  - RFC 2647/3511
  - RFC 4814
  - and that's *without* IP routing or QOS
  - 802.1D/802.1w STP
  - 802.1p/Q VLANs
  - 802.1X authentication
  - 802.3ab LLDP
  - 802.3ad link agg
  - 802.3af POE
- 
- All this requires smarter tools, smarter testers



# Why is switch testing so hard?

---

- Corporate happytalk line:
  - “Users want security and manageability and foo\*”
- My theory:
  - “Asia Inc. will kill us on switching -- *we need differentiators*”

\*Technical term describing multiple vendor pipe-dream technologies

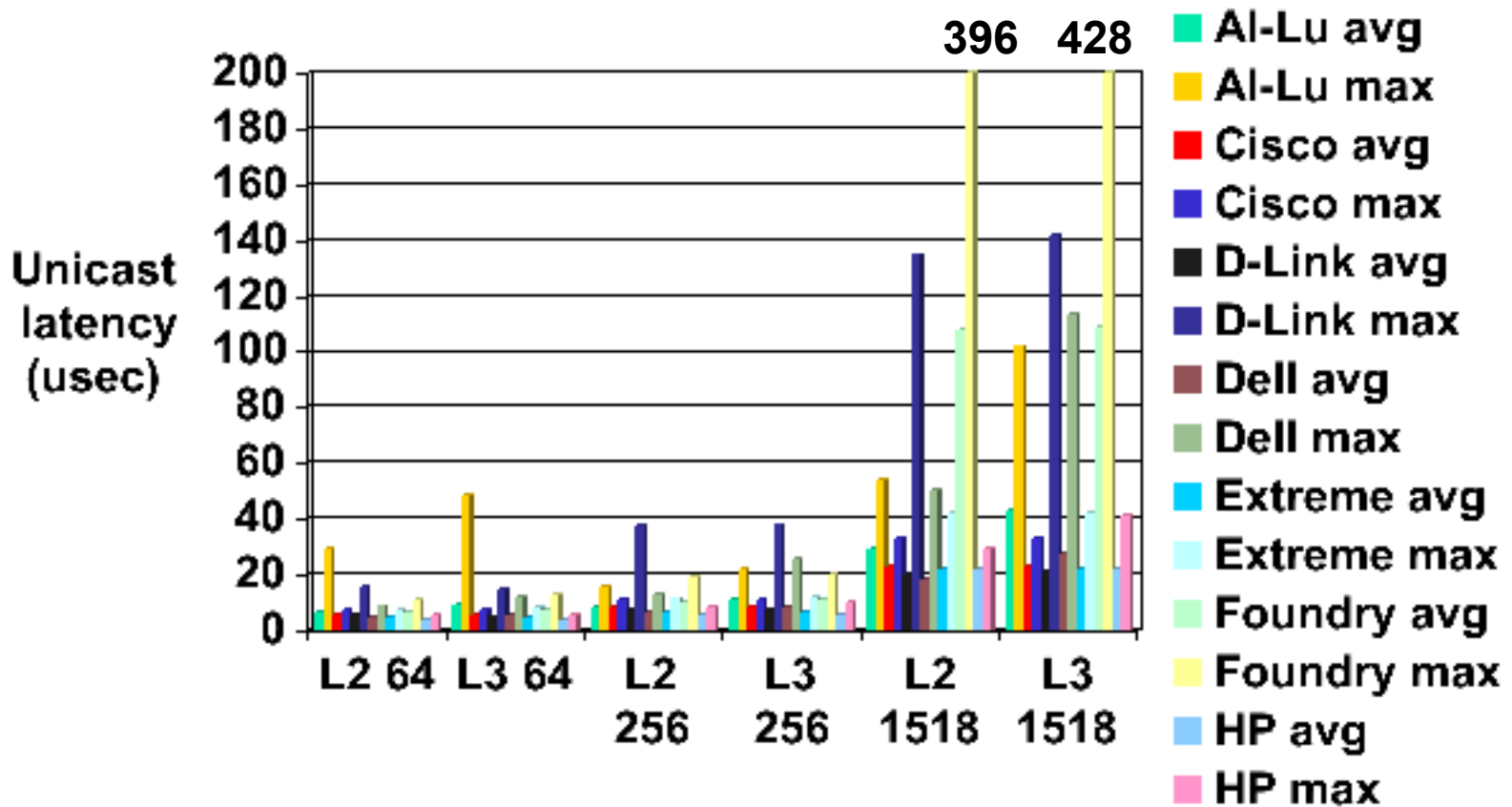


# Bye-bye, KISS principle

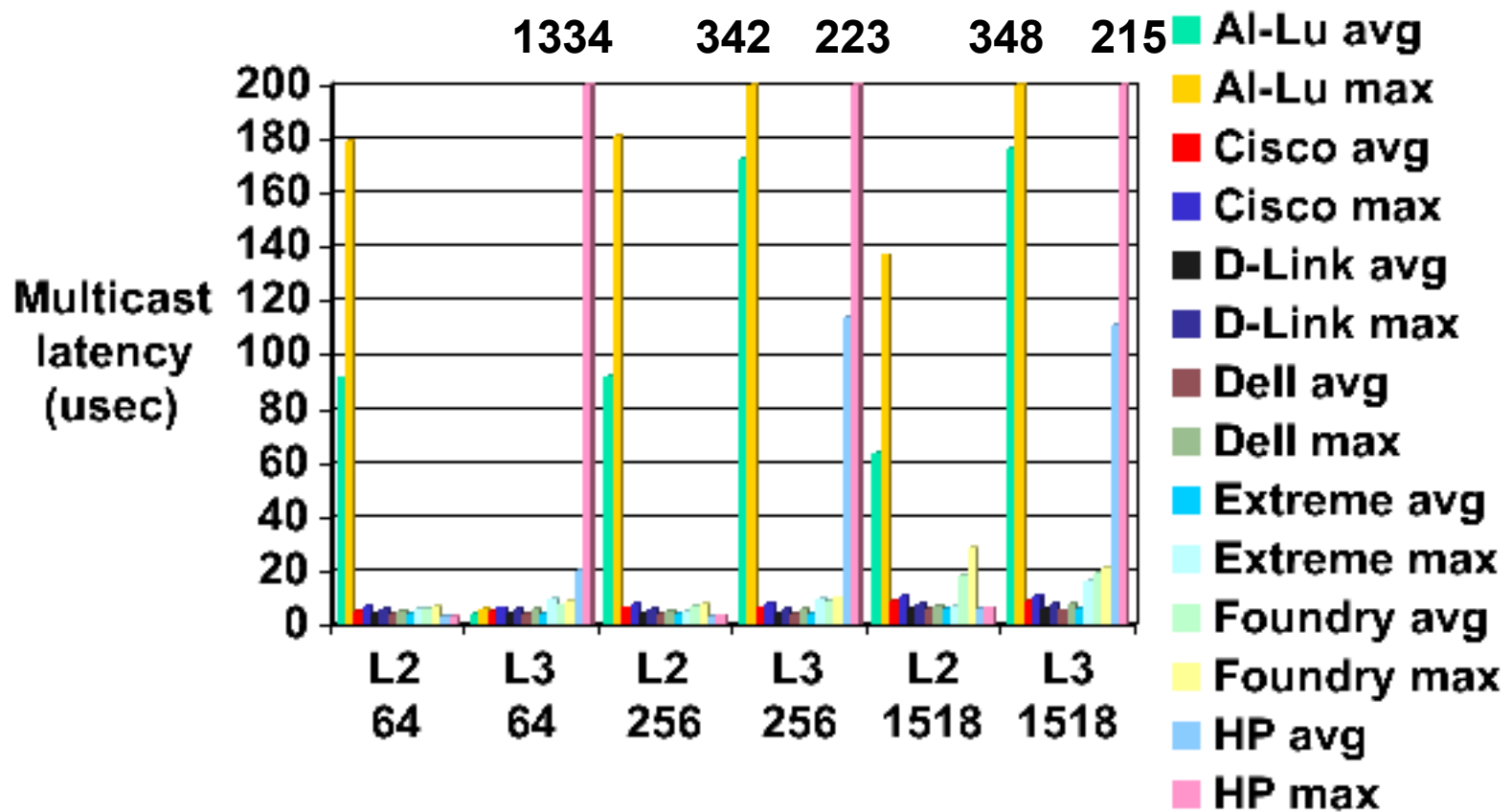
---

- Newest parts of any system tend to be the least trustworthy/stable
- For switches, that means:
  - IP multicast
  - Security
  - IPv6

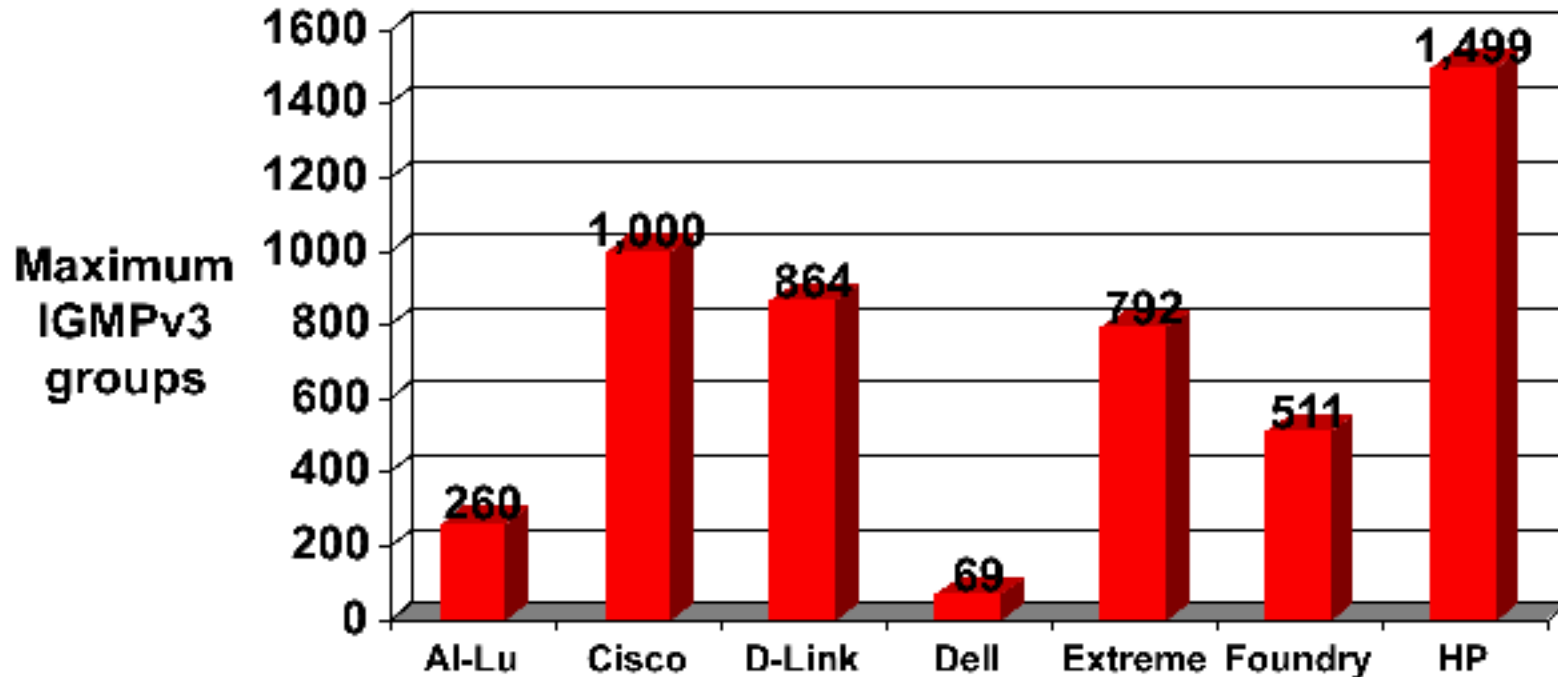
# Latency and jitter still matter



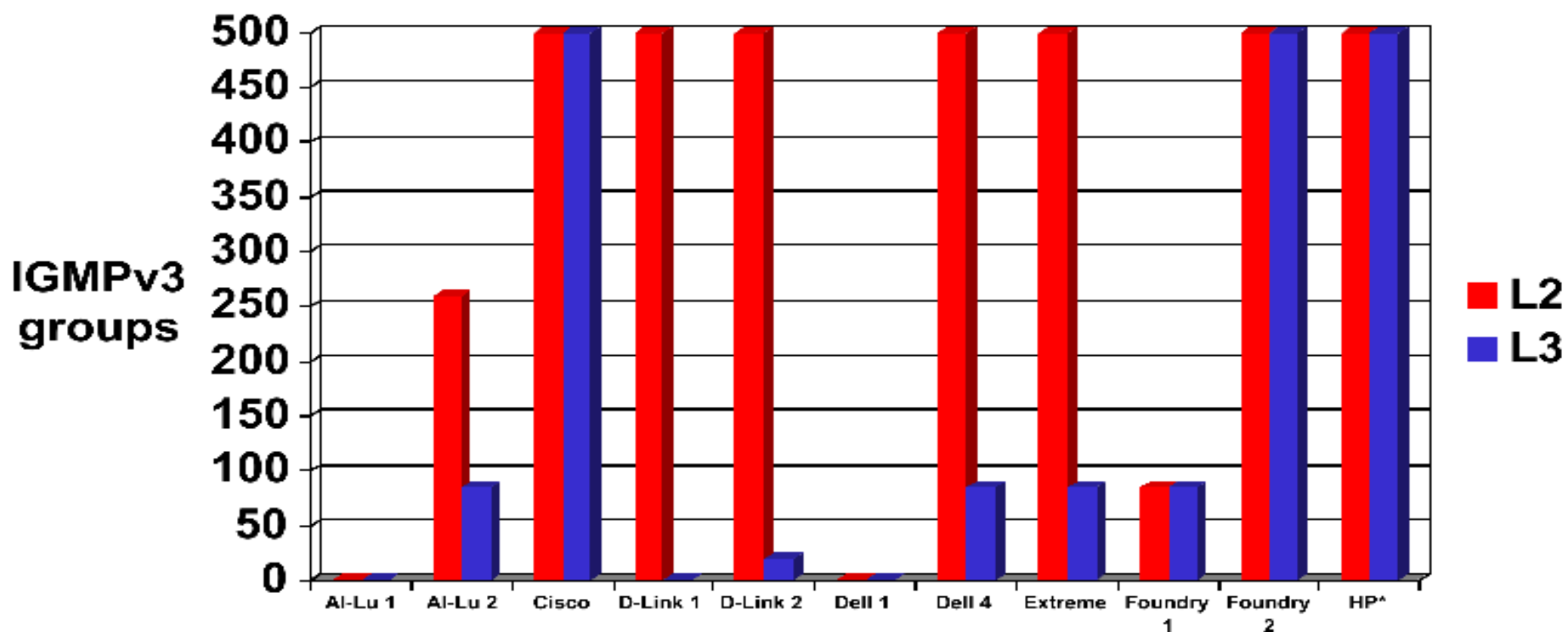
# Latency and jitter still matter



# Multicast group capacity is all over the place, part I



# Multicast group capacity is all over the place, part II



\*L3 used 2 VLANs/subnets/PIM routers; all others used 49



# About access control

---

- NAC is complicated...
  - Multiple flavors,  
each with multiple sublayers
- ...but the basic idea is simple
  - Who you are governs where you can go

# About access control

- We only looked at 802.1X authentication

Authentication server



Juniper  
Steel-Belted Radius  
Enterprise Edition 6.1

Authenticator



Suplicants





# About access control

---

- Six scenarios
  - One user, auth works, static VLAN
  - Two users, auth works, static VLAN
  - One user, auth works, dynamic VLAN
  - One user, auth works dynamic ACL
  - One user, auth fails, guest VLAN
  - One user, no 802.1X (e.g., printer)



# 802.1X scorecard

|                     | Al-Lu | D-Link | Cisco | Dell | Extreme | Foundry | HP    |
|---------------------|-------|--------|-------|------|---------|---------|-------|
| <b>One user</b>     | Pass  | Pass   | Pass  | Pass | Pass    | Pass    | Pass  |
| <b>Two users</b>    | Pass  | Pass   | Fail  | Fail | Pass    | Pass    | Pass  |
| <b>Dynamic VLAN</b> | Pass  | Pass   | Pass  | Fail | Pass    | Pass    | Pass  |
| <b>Dynamic ACL</b>  | Fail  | Fail   | Pass  | Fail | Pass    | Pass    | Pass* |
| <b>Guest VLAN</b>   | Pass  | Pass   | Pass  | Pass | Pass    | Pass    | Pass  |
| <b>MAC fallback</b> | Pass  | Fail   | Pass  | Fail | Pass    | Pass    | Pass  |

\*Shhh! Only with secret undocumented syntax



# 802.1X results

---

- Multi-auth failures are most troubling
  - “Badge tailgating” metaphor
  - False sense of security
  - It’s a protocol violation, but...
    - ...real-world use cases exist
      - IP phone
      - Conference room with one drop and a hub
      - WLAN access point

# Management methods: IPv4

|                      | Al-Lu   | Cisco   | D-Link | Dell | Extreme    | Foundry | HP  |
|----------------------|---------|---------|--------|------|------------|---------|-----|
| Secure factory reset | No (1)  | Yes     | Yes    | Yes  | No (1) (2) | Yes     | Yes |
| Default telnet       | Yes (3) | Yes     | Yes    | Yes  | Yes        | Yes     | Yes |
| Disable telnet       | Yes     | Yes     | Yes    | Yes  | Yes        | Yes     | Yes |
| Default HTTP         | Yes (3) | Yes     | Yes    | Yes  | No         | Yes     | Yes |
| Disable HTTP         | Yes     | Yes     | Yes    | Yes  | Yes        | Yes     | Yes |
| Default HTTPS        | Yes (3) | Yes     | No     | No   | No         | No      | No  |
| Enable HTTPS         | Yes     | Yes     | Yes    | Yes  | Yes        | Yes     | Yes |
| Default syslog       | No      | No      | No     | No   | No         | No      | No  |
| Enable syslog        | Yes     | Yes     | Yes    | Yes  | Yes        | Yes     | Yes |
| Default SSHv2        | Yes (3) | No      | No     | No   | No         | No      | No  |
| Enable SSHv2         | Yes     | Yes     | Yes    | Yes  | Yes        | Yes     | Yes |
| Default SSHv1        | No      | No      | No     | No   | No         | No      | No  |
| Allow SSHv1          | No      | Yes (4) | Yes    | No   | No         | No      | No  |

1. Doesn't reset administrative password
2. Doesn't remove SSH private key
3. Port answers but doesn't authenticate
4. Enabling SSH supports both version 1 and version 2, but SSHv1 can be disabled

# Management methods: IPv6

|                | Al-Lu   | Cisco   | D-Link | Dell    | Extreme | Foundry | HP      |
|----------------|---------|---------|--------|---------|---------|---------|---------|
| Default telnet | No      | No      | No     | N/A (7) | No      | No      | N/A (8) |
| Disable telnet | Yes     | Yes     | Yes    | N/A (7) | Yes     | Yes     | N/A (8) |
| Default HTTP   | No      | No      | No     | N/A (7) | No      | No      | N/A (8) |
| Disable HTTP   | Yes     | Yes     | Yes    | N/A (7) | No      | Yes     | N/A (8) |
| Default HTTPS  | No      | No      | No     | N/A (7) | No      | No      | N/A (8) |
| Enable HTTPS   | Yes     | Yes     | Yes    | N/A (7) | No      | Yes     | N/A (8) |
| Default syslog | No      | No (6)  | No     | N/A (7) | No      | No      | N/A (8) |
| Enable syslog  | Yes     | No      | No     | N/A (7) | No      | Yes     | N/A (8) |
| Default SSHv2  | Yes (3) | No      | No     | N/A (7) | No      | No      | N/A (8) |
| Enable SSHv2   | Yes     | Yes     | Yes    | N/A (7) | Yes     | Yes     | N/A (8) |
| Default SSHv1  | No      | No      | No     | N/A (7) | No      | No      | N/A (8) |
| Allow SSHv1    | No      | Yes (5) | No     | N/A (7) | No      | No      | N/A (8) |

3. Port answers but doesn't authenticate
4. Default is to enable telnet, but warns user that telnet is insecure
5. Enabling SSH supports both version 1 and version 2, but SSHv1 can be disabled
6. Software version tested does not support syslog over IPv6; Cisco says this is supported in current shipping version 12.2(44)SE.
7. Does not support management over IPv6
8. Software version tested did not support IPv6 on default VLAN; HP says this is supported in current shipping version 13.x.



# Future trends in switch testing

---

- Density wars are heating up again
  - Next sweet spot: 128-512 10G ports
- Virtualization
- Storm control
- Wired/wireless convergence
- 40G and 100G are coming
- Teaching L2 folks about L4 and L7



# Does price matter?

---

- Yes
  - We all have budgets
  - Nearly 6X spread between lo and hi
    - Dell, \$5,779; Cisco, \$33,980
- No
  - US list prices are, uh, squishy
  - *Network World* articles reprinted worldwide
  - We told vendors we wouldn't use price



# Thanks!

---

- [dnewman@networktest.com](mailto:dnewman@networktest.com)
- Methodology
  - <http://networktest.com/10g07/10g07meth.html>
- This preso:
  - In the conference materials

**networktest**