IPv6 Network Security

LSU

LOUISIANA STATE UNIVERSITY

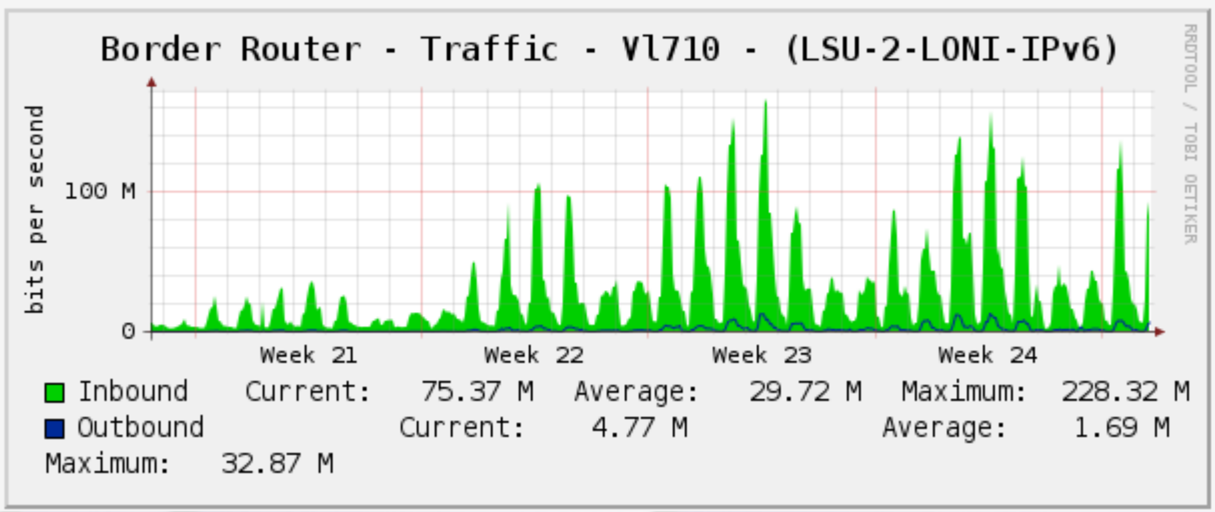
its-security@lsu.edu

IPv6

- Raising awareness about IPv6
- IPv6 Basics
- Windows notes
- Windows Firewall Demo
- Linux(RHEL) Firewall Demo
- [Mac OS 10.7 Lion Firewall Notes]
- [AAAA record via IPControl]

World IPv6 Launch

June 6, 2012
Traffic increase



IPv6 Accessible Sites at LSU

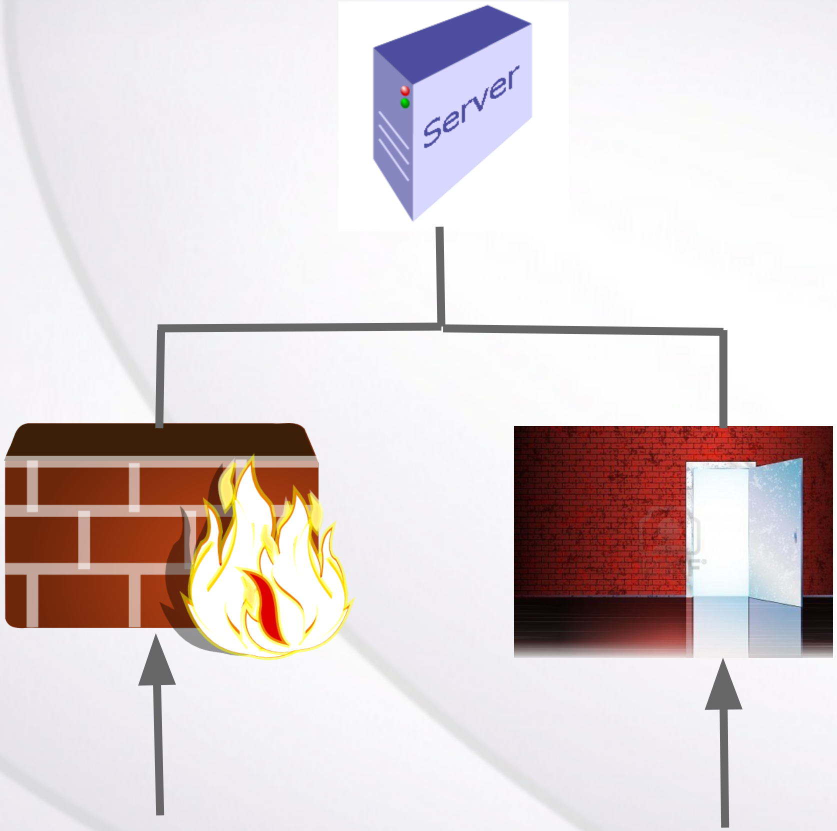
- www.lsu.edu
- www.law.lsu.edu
- www.eng.lsu.edu
- www.pete.lsu.edu
- grok.lsu.edu
- tigerware.lsu.edu
- connect.lsu.edu

The good news

- With IPv6 First-hop security
  - More difficult to go rogue
  - Block rogue router advertisements
  - Block rogue DHCP servers

- Very difficult for attacker to sweep the network

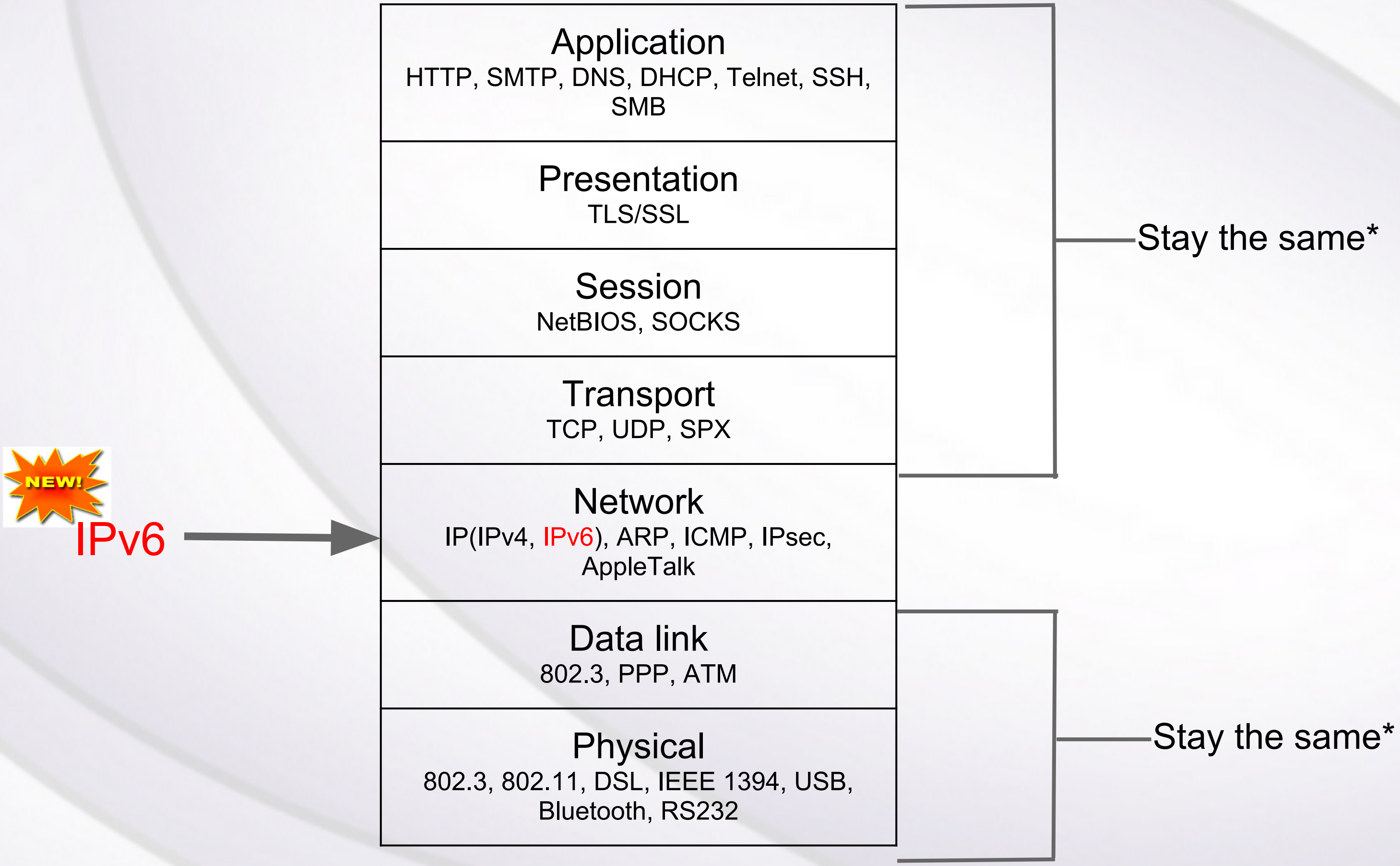
Current State



IPv4

IPv6

What's changing?



Application
HTTP, SMTP, DNS, DHCP, Telnet, SSH, SMB

Presentation
TLS/SSL

Session
NetBIOS, SOCKS

Transport
TCP, UDP, SPX

Network
IP(IPv4, IPv6), ARP, ICMP, IPsec, AppleTalk

Data link
802.3, PPP, ATM

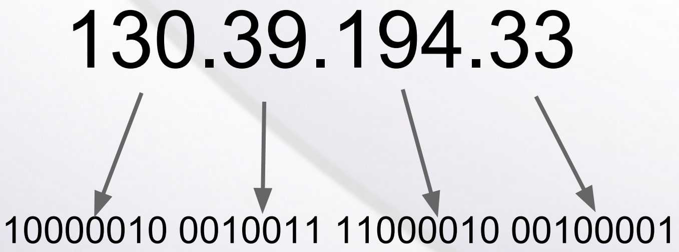
Physical
802.3, 802.11, DSL, IEEE 1394, USB, Bluetooth, RS232

*more or less

Looking Back

IPv4 Addressing scheme:

- 32-bit addresses, split into four, 8-bit blocks
- Therefore, each block has a value from 0 to 255



130.39.194.33

10000010 0010011 11000010 00100001

IPv6

- 128-bit addressing scheme
- Represented as 32 hexadecimal numbers in 8 blocks of 4 numbers.
- Each hexadecimal digit represents four bits and range from 0 to F in value.

2620:0105:b000:2180:949b:072c:127a:e814

IPv6 Address Shorthand

- Leading zeroes may be omitted
  - 2001:0db8:85a3:0000:0000:8a2e:0370:7334

    ↓

  - 2001:db8:85a3:0:0:8a2e:370:7334

IPv6 Address Shorthand

- Two or more consecutive blocks of zeros may be replaced with two colons ::
  - 2001:0db8:85a3:0000:0000:8a2e:0370:7334
  - 2001:db8:85a3::8a2e:370:7334
  - but not a single block:
  - 2001:db8:0000:1:1:1:1:1
  - 2001:db8:0:1:1:1:1:1

IPv6 Address Shorthand

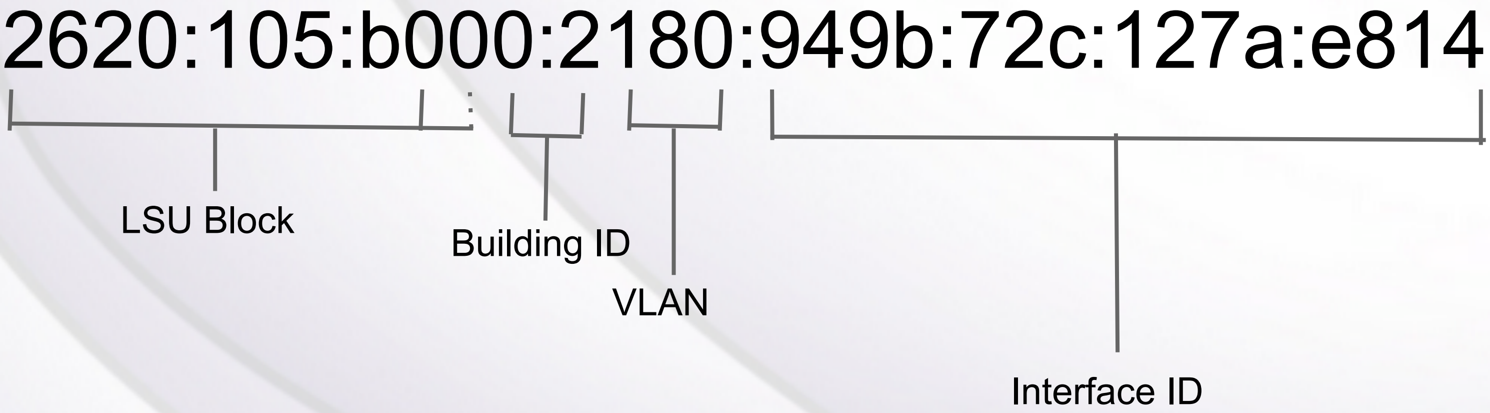
- Compress leftmost zero groups
  - 2001:0db8:0000:0000:0001:0000:0000:0001
  - 2001:db8::1:0:0:1
  - Not valid: 2001:db8:0:0:1::1
  - Can only compress ONCE
  - Not valid: 2001:db8::1::1
- Use lower-case letters
- Shorten as much as possible

IPv6 @ LSU

- Dual stack network
- Every machine has an IPv4 and IPv6 address
- Address Space: 2620:105:b000::/40
- Automatic assignment using EIU-64
- No support for tunneling(6to4, Teredo, ISATAP)

IPv6 Address

bits	48 or more	16 or fewer	64
field	routing prefix	subnet ID	Interface ID



2620:105:b000:2180:949b:72c:127a:e814

LSU Block

Building ID

VLAN

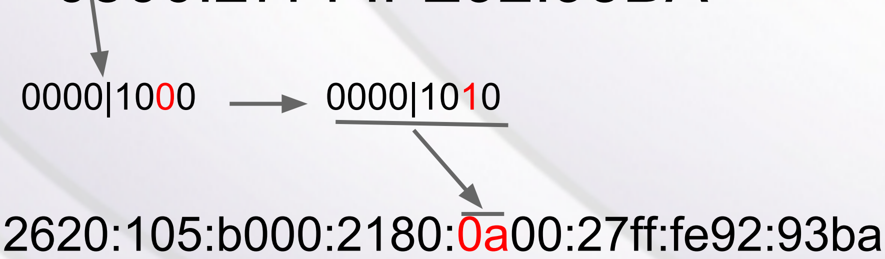
Interface ID

Interface ID

- LSU uses modified EIU-64 for stateless address autoconfiguration
- Based on the 48-bit MAC address
- For privacy, some operating systems generate a random 48-bit address
- LSU is currently looking into DHCPv6 as a replacement

Interface ID - EIU-64

- Take a 48-bit MAC address:
  - 08:00:27:92:93:BA
  - Insert FF:FE in the middle
  - 0800:27FF:FE92:93BA
  - Invert the seventh bit from the left.
  - 0800:27FF:FE92:93BA



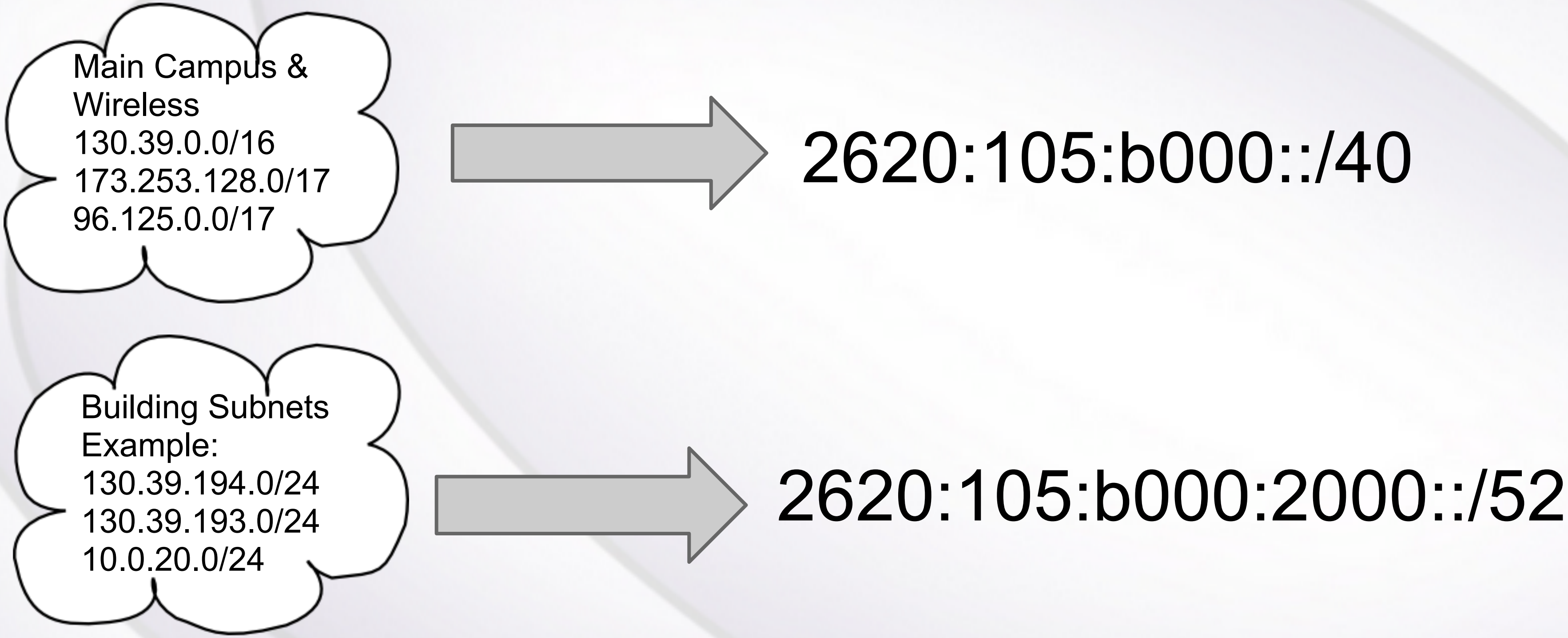
0000|1000 → 0000|1010

2620:105:b000:2180:0a00:27ff:fe92:93ba

Notable IPv6 Address Spaces

- Unspecified ::/128
- Loopback: ::1/128
- Unique local: fc00::/7
- Link-local: fe80::/10
- Multicast: ff00::/8

IPv4 equivalent spaces



Main Campus &
Wireless
130.39.0.0/16
173.253.128.0/17
96.125.0.0/17

2620:105:b000::/40

Building Subnets
Example:
130.39.194.0/24
130.39.193.0/24
10.0.20.0/24

2620:105:b000:2000::/52

Even more restrictive

- Match building ID and VLAN:
  - 2620:105:b000:2180::/64
- Finally, specific host:
  - 2620:105:b000:2180:221:86ff:fe24:6d34/128

Windows Disabling Tunnelling

- Manually:
  - netsh interface teredo set state disabled
  - netsh interface ipv6 6to4 set state state=disabled undoonstop=disabled
  - netsh interface ipv6 isatap set state state=disabled
- Easy way:
  - http://support.microsoft.com/kb/929852

Windows 7 Temporary IPv6 Address

- For privacy, Windows 7 also generates a random IPv6 address that changes often:
  - Every Windows 7 machine has 3 IPv6 Addresses
    - Fixed global
    - Temporary global
    - Link-Local
- Temporary address is used for actual IPv6 communications
- Could be a problem for firewall rules
  - netsh int ipv6 set privacy disabled
  - reboot

Windows Firewall Demo

- Unified both protocols
- Very simple
- Must specify both IPv4 and IPv6 scopes

Linux Firewall Demo(ip6tables)

- Very similar to iptables for IPv4
  - Support for NAT and redirections are in the works
- Make sure ip6tables service is set to run on system startup(runlevels 2 to 5):
  - chkconfig --list | grep ip6tables
  - if not: chkconfig ip6tables on
- Configuration file:
  - /etc/sysconfig/ip6tables
  - Be careful, system-config-firewall may overwrite your changes
  - Restart ip6tables service after changes are made:
  - service ip6tables restart

Sample

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p ipv6-icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp6-adm-prohibited
-A FORWARD -j REJECT --reject-with icmp6-adm-prohibited
COMMIT
```

ip6tables

Open port 80:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
```

Restrict port 80 to campus only:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -s 2620:105:b000::/40 -j ACCEPT
```

Restrict port 80 to building subnets:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -s 2620:105:b000:2000::/52 -j ACCEPT
```

ip6tables

Restrict port 80 to building subnets and VLAN:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -s 2620:105:b000:2180::/64 -j ACCEPT
```

Allow only a particular IPv6 Address:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -s 2620:105:b000:8500:250:56ff:fea4:63/128 -j ACCEPT
```

Block subnet:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -s 2620:105:b00b:4800::/64 -j DROP
```

Mac OS X Notes

- Also uses temporary IPv6 address
  - sysctl net.inet6.ip6.use_tempaddr=0
- By default, Mac OS X firewall is OFF
  - Remember to enable firewall after OS installation/upgrade

Mac OS X firewall (pf)

- The GUI firewall is an application firewall
  - Rules are based on applications instead of ports or IP addresses
  - Free front end for pf (IceFloor):
    - http://www.hanynet.com/icefloor
    - Application firewall does not override pf rules

- Please see me after presentation if you're running OS X server.

Thank you!

Next topic?

Anybody?