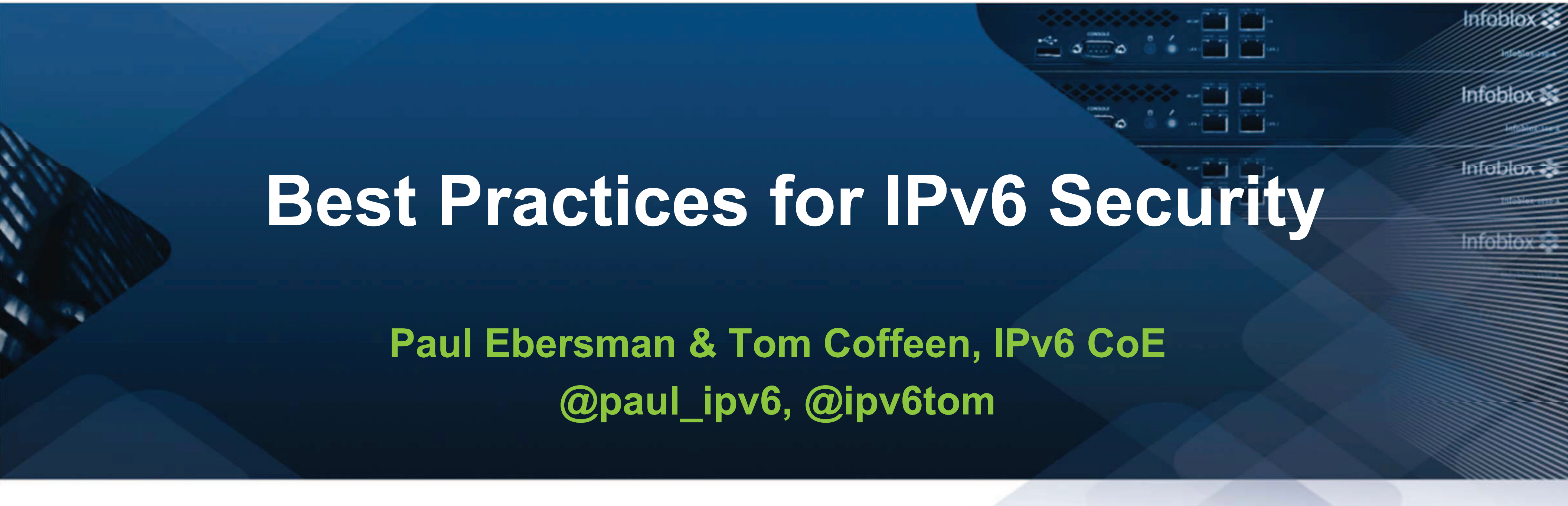


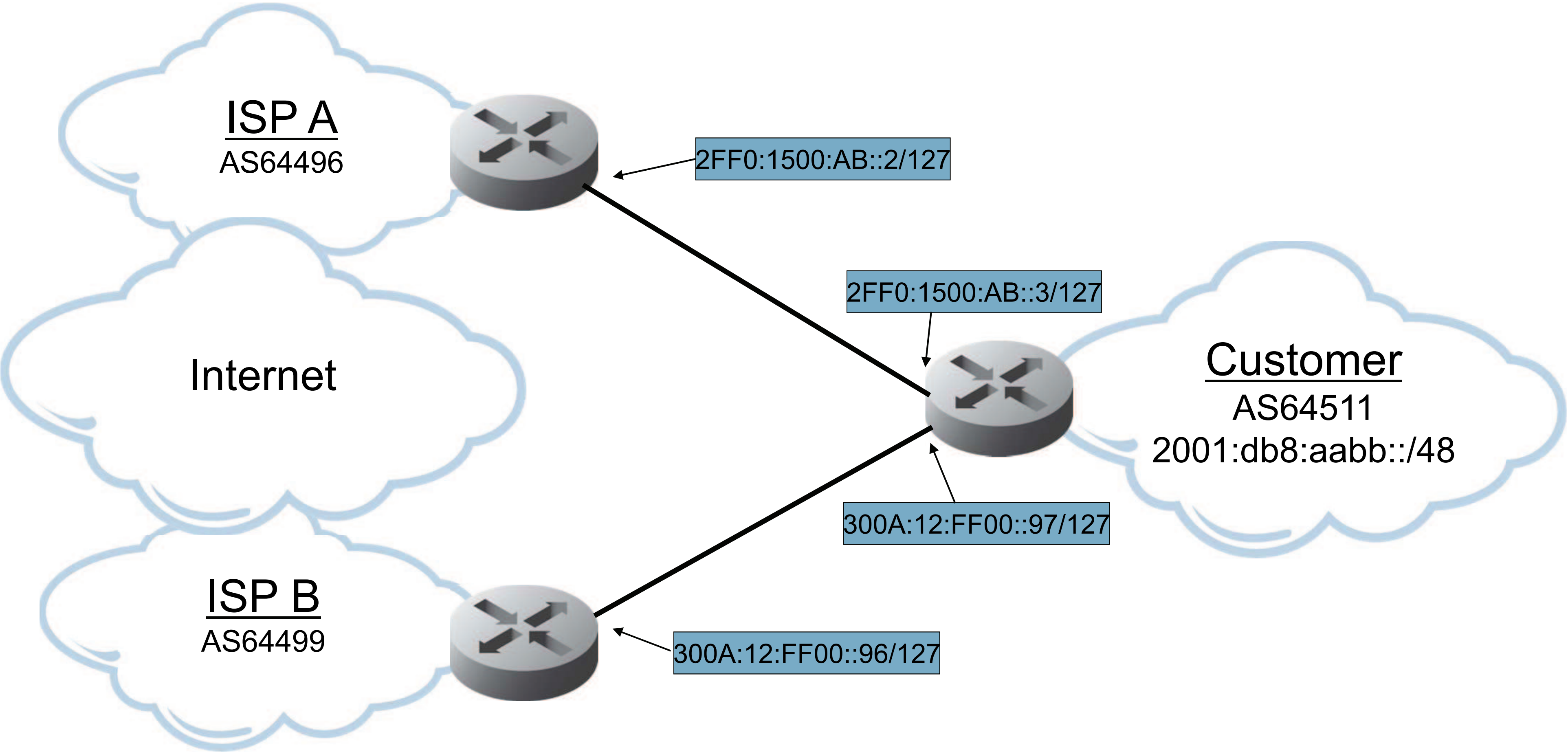
# Best Practices for IPv6 Security

Paul Ebersman & Tom Coffeen, IPv6 CoE
@paul_ipv6, @ipv6tom

# Connecting to your provider

# Connecting to your provider

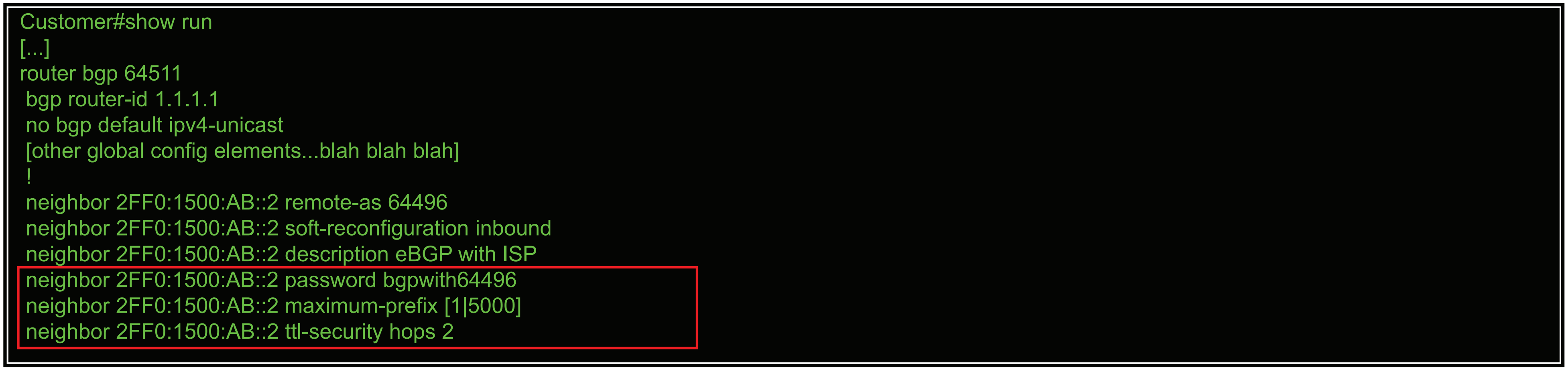
- **Use /127s for point-to-point links (RFC 6164)**
  - Avoids potential ping-pong and neighbor cache exhaustion attacks
  - Allocate an entire /64 for each link but configure with a /127



©2012 Infoblox Inc. All Rights Reserved.

# Connecting to your provider

- **IPv6 BGP4+ peering security**
  - MD5 passwords
  - TTL Security command
  - Max prefix command
  - Multiprotocol BGP

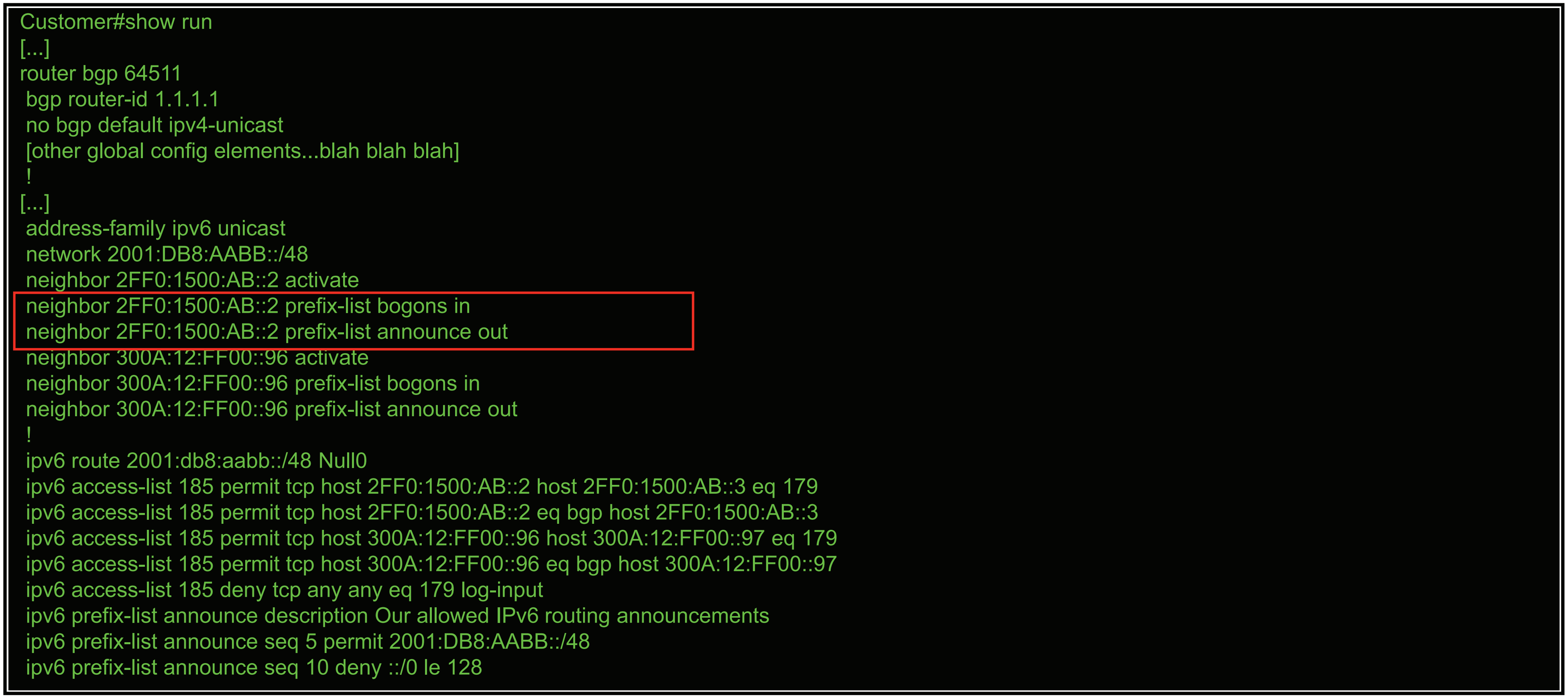


```
Customer#show run
[...]
router bgp 64511
 bgp router-id 1.1.1.1
 no bgp default ipv4-unicast
 [other global config elements...blah blah blah]
 !
 neighbor 2FF0:1500:AB::2 remote-as 64496
 neighbor 2FF0:1500:AB::2 soft-reconfiguration inbound
 neighbor 2FF0:1500:AB::2 description eBGP with ISP
 neighbor 2FF0:1500:AB::2 password bgpwith64496
 neighbor 2FF0:1500:AB::2 maximum-prefix [1|5000]
 neighbor 2FF0:1500:AB::2 ttl-security hops 2
```

© 2012 Infoblox Inc. All Rights Reserved.

# Connecting to your provider

- **BGP prefix filtering**
  - Similar configuration elements to IPv4 BGP prefix filtering
  - IPv6 “Bogons” greatly outnumber valid IPv6 prefixes
  - Explicitly allow known good prefixes and implicitly deny everything else



```
Customer#show run
[...]
router bgp 64511
 bgp router-id 1.1.1.1
 no bgp default ipv4-unicast
 [other global config elements...blah blah blah]
 !
[...]
 address-family ipv6 unicast
 network 2001:DB8:AABB::/48
 neighbor 2FF0:1500:AB::2 activate
 neighbor 2FF0:1500:AB::2 prefix-list bogons in
 neighbor 2FF0:1500:AB::2 prefix-list announce out
 neighbor 300A:12:FF00::96 activate
 neighbor 300A:12:FF00::96 prefix-list bogons in
 neighbor 300A:12:FF00::96 prefix-list announce out
 !
 ipv6 route 2001:db8:aabb::/48 Null0
 ipv6 access-list 185 permit tcp host 2FF0:1500:AB::2 host 2FF0:1500:AB::3 eq 179
 ipv6 access-list 185 permit tcp host 2FF0:1500:AB::2 eq bgp host 2FF0:1500:AB::3
 ipv6 access-list 185 permit tcp host 300A:12:FF00::96 host 300A:12:FF00::97 eq 179
 ipv6 access-list 185 permit tcp host 300A:12:FF00::96 eq bgp host 300A:12:FF00::97
 ipv6 access-list 185 deny tcp any any eq 179 log-input
 ipv6 prefix-list announce description Our allowed IPv6 routing announcements
 ipv6 prefix-list announce seq 5 permit 2001:DB8:AABB::/48
 ipv6 prefix-list announce seq 10 deny ::/0 le 128
```

©2012 Infoblox Inc. All Rights Reserved.

# Securing Routers and Switches

# Securing Routers and Switches

- **Device access**
  - Explicitly allow the following over IPv6 where appropriate:
    - SSH (please, disable Telnet)
    - SNMP
    - FTP/TFTP
    - NTP/SNTP
  - Remember, ICMPv6 is a special case

- **Interface security**
  - Configure ‘no ipv6 redirects’ and ‘no ipv6 unreachables’
  - Configure RA Guard

© 2012 Infoblox Inc. All Rights Reserved.

# Firewalls and Security

# Security Appliances - Firewalls, IDS, and IPS

- **IDS/IPS**
  - Persistent issues with many vendor’s IPv4/IPv6 feature parity
- **Firewall policy/ACLs**
  - Don’t reflexively copy existing IPv4 ACL policy for use with IPv6
    - A minimally sufficient IPv6 policy with the least number of ACL entries may be best

**IPv4 Policy**

| Rule | Source | Destination | Protocol | Action |
|---|---|---|---|---|
| 1 | Any-IPv4 | V4-web-1 | HTTP & HTTPS | **Permit** |
| 2 | Any-IPv4 | Any-IPv4 | Any | **Deny** |

**IPv6 Policy**

| Rule | Source | Destination | Protocol | Action |
|---|---|---|---|---|
| 1 | Any-IPv6 | V6-web-1 | HTTP & HTTPS | **Permit** |
| 2 | Any-IPv6 | Any-IPv6 | Any | **Deny** |

©2012 Infoblox Inc. All Rights Reserved.

# Security Appliances - Firewalls, IDS, and IPS

- **Firewall policy/ACLs**
  - Will your naming conventions survive the eventual deprecation of IPv4?

| Rule | Source | Destination | Protocol | Action |
|---|---|---|---|---|
| 1 | Any-IPv4<br>Any-IPv6 | V4-Web-1<br>V6-Web-1 | HTTP &<br>HTTPS | **Permit** |
| 2 | Any-IPv4<br>Any-IPv6 | DNS | TCP 53<br>UDP 53 | **Permit** |
| 3 | Any-IPv4<br>Any-IPv6 | V4-FTP-2<br>V6-FTP-2 | FTP | **Permit** |
| 4 | Any-IPv4<br>Any-IPv6 | V4-Mail-1<br>V6-Mail-1 | SMTP | **Permit** |
| 5 | Any-IPv4<br>Any-IPv6 | Any-IPv4<br>Any-IPv6 | ICMPv6 | **Permit** |
| 6 | Any | Any | Any | **Deny** |

  - Disable IPv6 tunneling
  - Treat ICMPv6 with care

©2012 Infoblox Inc. All Rights Reserved.

# Securing Hosts and Servers

# Securing Hosts and Servers

- **Host security**
  - The use of IPv6 GUA (i.e., “public”) addresses on enterprise networks requires greater emphasis on host security
- **Steps to secure hosts and servers**
  - Validate host firewall support for IPv6
  - Block potentially malicious IPv6 packets at the host level (you’re doing that already in IPv4, right?)
  - Explicitly disable IPv6 tunneling
  - Explicitly enable listening only on appropriate ports
  - If necessary, explicitly disable IPv6 forwarding
- **Privacy addresses**
  - Often on by default but problematic where tight host management is desired

© 2012 Infoblox Inc. All Rights Reserved.

Infoblox®

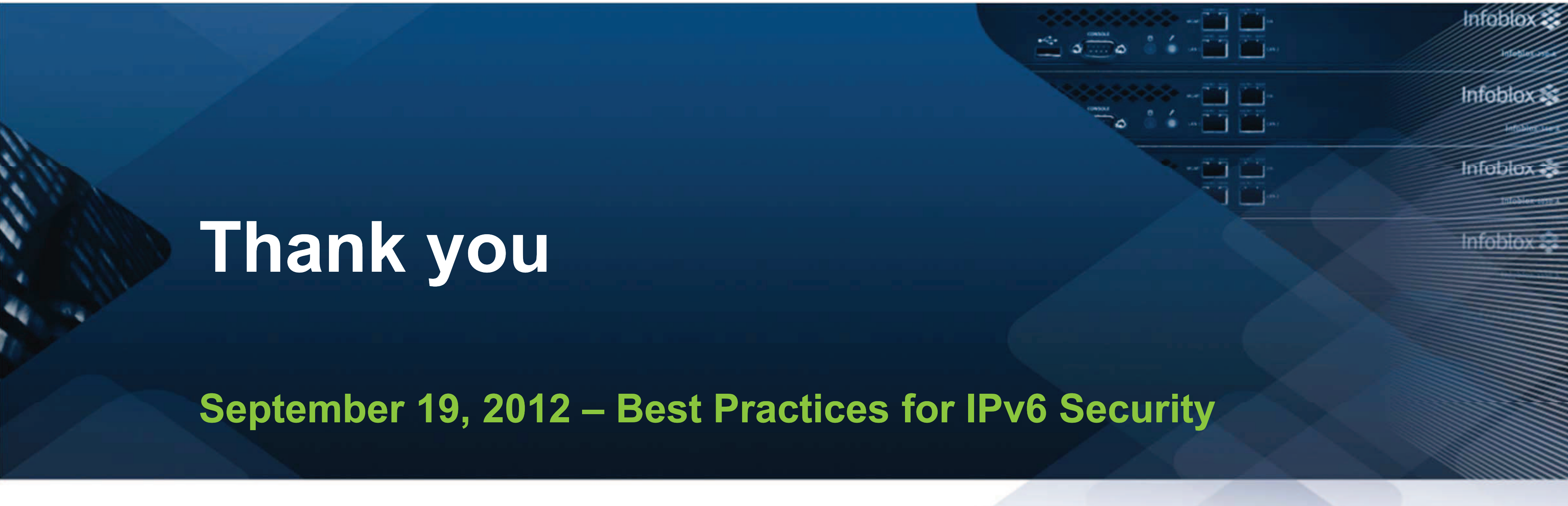
# Questions?

# Thank you for attending!

- **bloxHub – Infoblox Technical Community**
  - Visit this page for a complete Q&A transcript http://www.infoblox.com/community/forum/netmri/general-discussions/ipv6-security-webinar-discussion
  - 1st 100 people who post a relevant question will receive a T-shirt or hat

- **Visit Infoblox.com for more info on upcoming events**
  - Twitter @Infoblox

- **Upcoming Live Events**
  - October 9th-11th: VMworld, Barcelona
  - October 14th-18th: GITEX, Dubai
  - October 17th-18th: IP Expo, London



# Thank you

**September 19, 2012 – Best Practices for IPv6 Security**