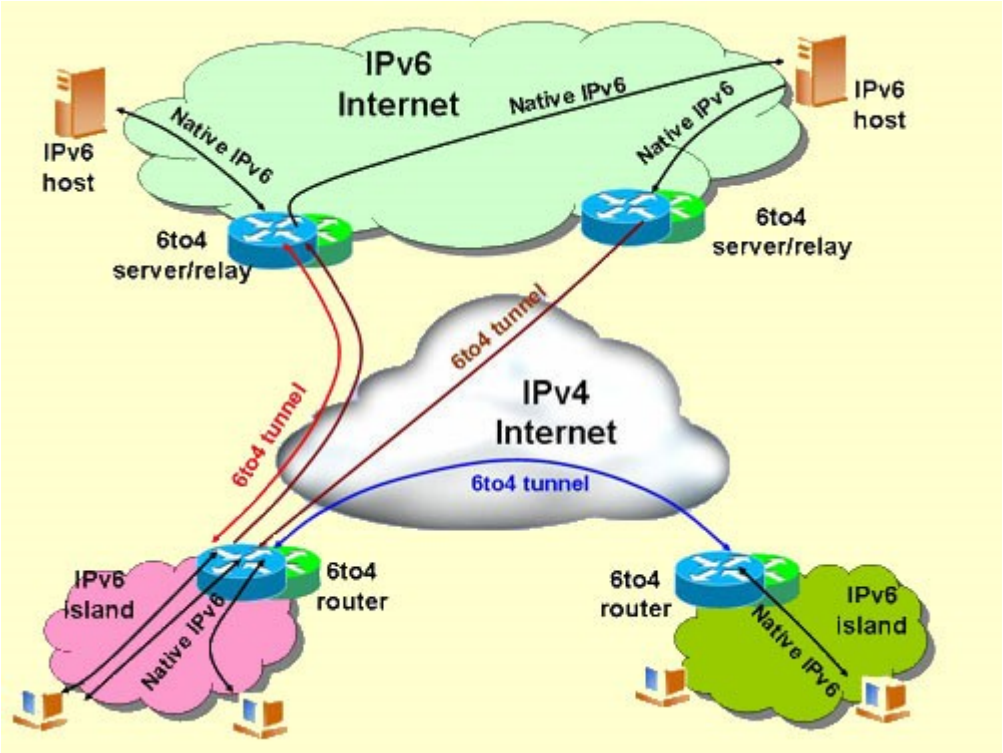
CSCD 433/533
Advanced Networks
Spring 2016

Lecture 20
IPv6 and Tunnels
IpSec and Security



Topics

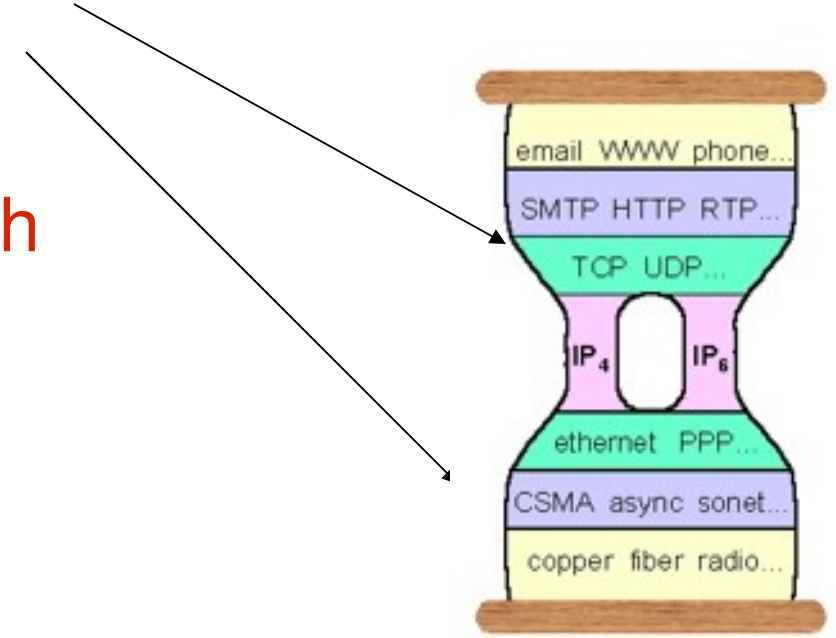
- Ipv4 Stop-gap methods to save it
- Ipv6
  - What is it?
  - When is it coming?
  - How does it differ from Ipv4?

- Transition to Ipv6
- Mechanisms
- Ipv6 and Security

IPv4

- Said it was the “glue” of the Internet
- Allows everything
  under it and many things over it
  in terms of protocols

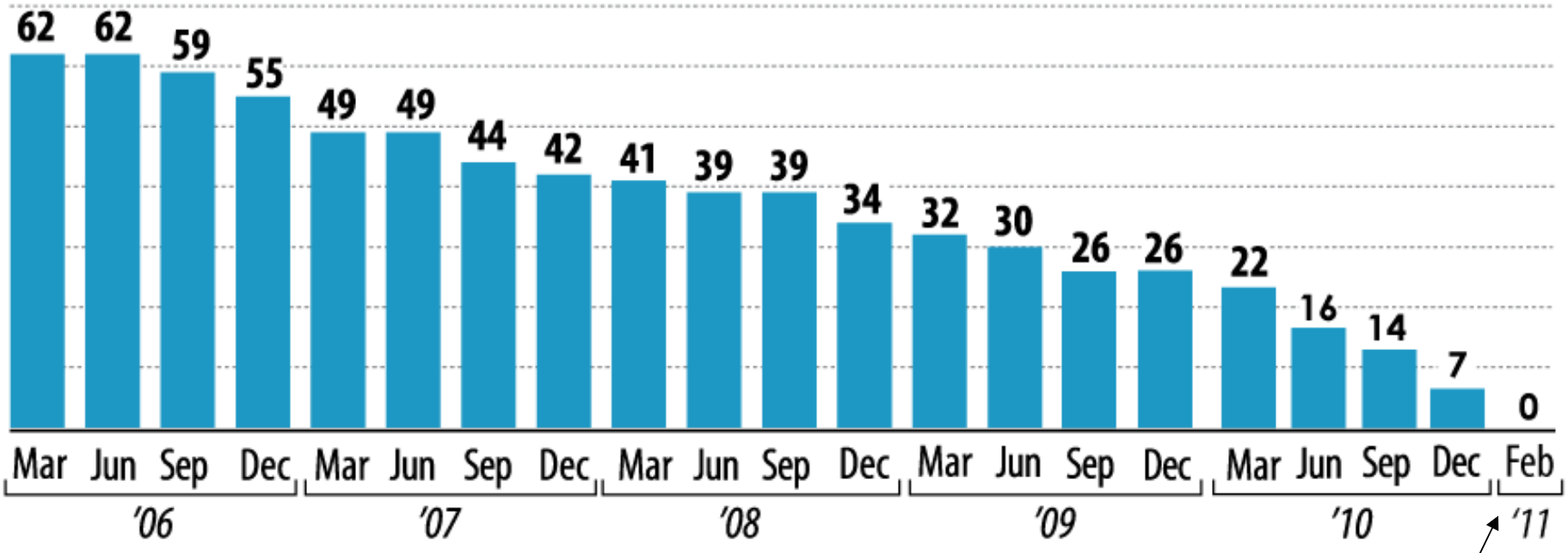
What is one problem with Ipv4?



Ipv6 Motivation and Background

- IPv4 Supports about 4 billion IP Devices
  - IPv4 addressing scheme did not expect recent exponential growth of the Internet
  - Many regions undergoing substantial growth in IP address utilization such as Asia and Europe
  - IPv4 space will be exhausted by 20??
  - **Did that happen???**

Available IPv4 Space in /8s



Yes! Feb 2011

IPv4 Depletion Situation Report

- Each RIR received its last /8 from IANA on February 3, 2011.
- IANA free pool of IPv4 addresses has reached 0%
- While each RIR currently has IPv4 addresses to allocate, it is impossible to predict when each RIR will run out
- ARIN publishes an inventory of available IPv4 addresses, updated daily, at **www.arin.net**

Latest stats
http://www.potaroo.net/tools/ipv4/index.html

ICANN Feb 3 2011 Event

The IANA IPv4 Address Free Pool is now Depleted

http://www.nro.net/media-center/video-archive-3-february-2011

Running out of Addresses

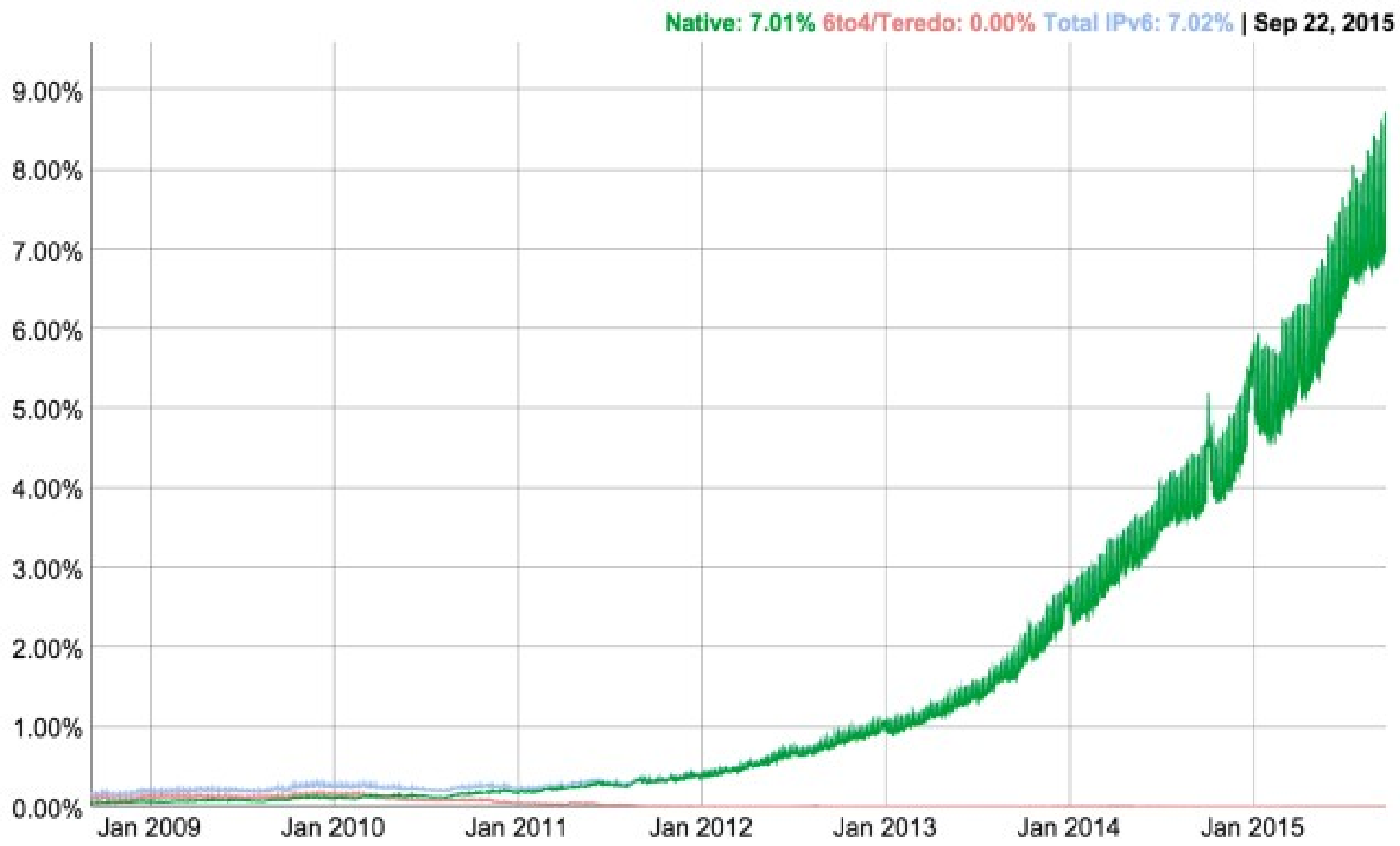
- These addresses could well be fully consumed within three to six months of that time at current rates of allocation
- APNIC was first RIR to exhaust its regional pool on 15 April 2011
- There is a small amount of address space reserved for the transition to IPv6, which will be allocated in a much more restricted way

In 2016 Ipv6 Adoption

2016 is the Year of IPv6

- 10% (10.41% on January 1, to be precise) of traffic hitting Google's servers – a pretty good indicator of overall Internet traffic – is coming from an IPv6 connection
- Verizon Wireless deployed IPv6 early and both they and T-Mobile USA have large IPv6 deployments
    - Encouraging to note that four major US mobile operators now all have measurable IPv6 deployments

10 Per Cent IPv6 in 2016



Developer Support for IPv6

- Apple http://blogs.unity3d.com/2016/05/10/unity-and-ipv6-support/
  - At WWDC 2015, announced that iOS 9 will support IPv6-only network services
  - All apps submitted to the App Store must support IPv6 starting in early 2016

  - Microsoft

    Microsoft is not so advanced

    https://technet.microsoft.com/en-us/network/hh994905.aspx

Ipv4 Address Preservation

Ipv4 Address Preservation

- Several techniques helped preserve address space
- Extended the addresses beyond the predicted exhaustion:
  - CIDR
  - NAT

Are we actively still doing both of these?

Methods to Salvage Address Space

- **Classless Interdomain Routing ...**
- CIDR is solution that helped with IP address allocation as well as routing table overflow
- What did this do?
  - Eliminated rigid class A, B, and C networks, replaced this with generalized "IP prefix"
  - Address assignments more closely fit an organization's specific needs
  - Didn't waste as many addresses

CIDR Review

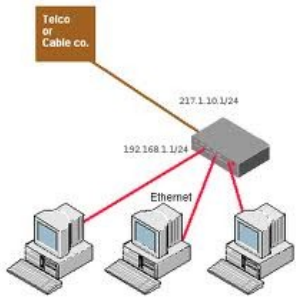
- How did they do this?
  - Allowed bits for network to be variable instead of fixed into strict categories
  - No longer had 8, 16 or 24 bits for network
    - Class A, B or C networks
  - Then, had to create variable length network masks to determine network size
    - Called, Variable Length Subnet Masks (VLSM) Example: 255.255.255.0
  - See next slide

CIDR Network Size / Number of Network Bits

- **Alternate way to specify CIDR networks is with the /n syntax**
  - **/n = number of network bits**

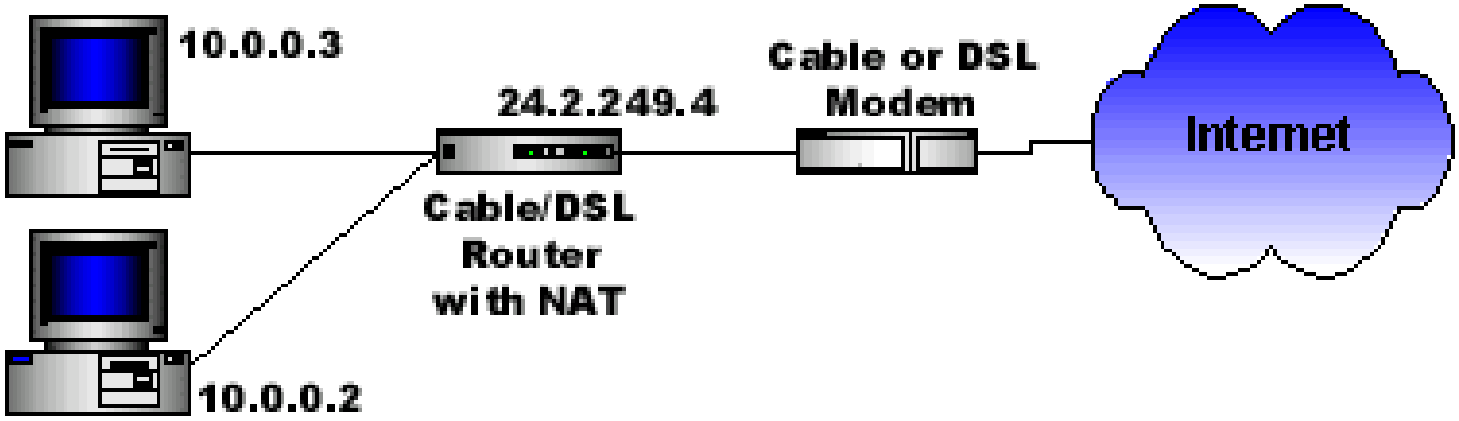
CIDR Block Prefix	# Equivalent Class C	# of Host Addresses
/27	1/8th of a Class C	32 hosts
/26	1/4th of a Class C	64 hosts
/25	1/2th of a Class C	128 hosts
/24	1 Class C	256 hosts
/23	2 Class C	512 hosts
/22	4 Class C	1,024 hosts
/21	8 Class C	2,048 hosts
/20	16 Class C	4,096 hosts
/19	32 Class C	8,192 hosts
/18	64 Class C	16,384 hosts
/17	128 Class C	32,768 hosts
/16	256 Class C	65,536 hosts

Network Address Translation (NAT)



- Network Address Translation (NAT)
  - Connect multiple computers to Internet,
  - With one IP address
  - Home users and small businesses connect their network to Internet cheaply
    - One address = Many computers
  - NAT used when number of IP addresses assigned to you by your ISP is less than number of computers that you wish to connect

NAT Advantages



- Advantage of NAT
  - Use one registered IP address for an entire network
  - Transparent to end systems mostly
  - Some Increased Security
    - Internal IP addresses Hidden
  - Delayed need for IPv4 replacement

NAT Disadvantages

Any Problems with NAT?

- Breaks end-to-end model !!!
- Increases management burden and complexity
- Breaks some applications
  - Games, VOIP, Encryption protocols ...
- Increases probability of mis-addressing
- Possible performance degradation
  - If you get close to the limit of about 25,000 connections

IPv6 the Next Implementation

IPv6 or IPng for Next Generation

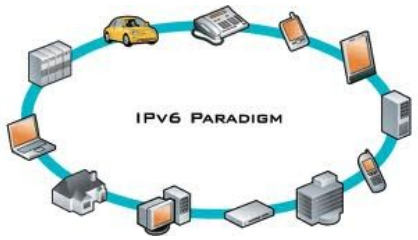
- IPv6 is "next generation" protocol
  - Created by **IETF,** Internet Engineering Task Force
  - IPv6 fixes a number of problems in IPv4
    - Limited IPv4 addresses
    - Lack of built-in security
    - Adds improvements to **Ipv4**
      - Routing and network auto configuration
    - **IPv6** expected to gradually replace **IPv4**, with two coexisting for a number of years during a transition period … which is NOW!

IPv6 Features

- **First and foremost:**
- Larger addresses,128-bit addresses
- Solves the address shortage (of course)
- Went from 2^{32} to 2^{128}

- Or approximately, roughly 295 addresses for each of roughly 6.5 billion people alive today
- Different perspective, this is 252 addresses for every observable star in known universe or
- 1,500 addresses /sq. foot of earth's surface

IPv6 Features - Same as Ipv4



- What has **not** changed from IPv4?
- Almost everything!
  - IPv6 still uses connectionless datagram delivery
  - Still uses end-to-end connections
  - Still supports TCP and UDP protocols
  - Allows multiple protocols and technologies under it
  - A lot like Ipv4

IPv6 Features - Different from Ipv4

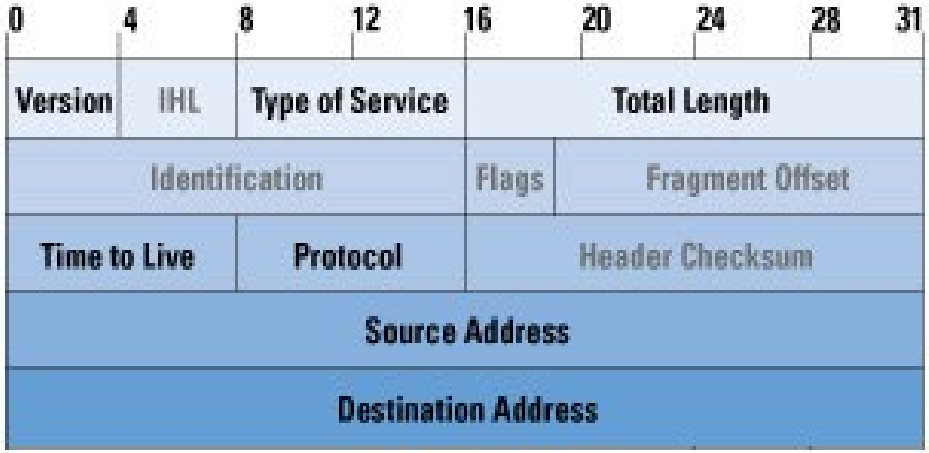
1. Simplified header format
   - IPv6, fixed length header, does not include most Ipv4 options
   - Has fixed length 40 bytes ... faster processing
   - Options dealt with in **extension headers**,
     - Only inserted after IPv6 header if needed
2. Address extended to 128 bits
3. New version of ICMPv6 !!!
   - Includes Neighbor Discovery, Autoconfiguration, Multicast Listener Discovery, Path MTU Discovery
4. Enhanced Security and QoS Features

About IPv4 and IPv6

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	1981	1999
Address	32-bit number	128-bit number
Size **Address Format**	Dotted Decimal Notation: 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00:0123:4567:8901:ABCD
Prefix	192.149.0.0/24	3FFE:F200:0234::/48
Notation **Number of Addresses**	2^{32} = 4,294,967,296	2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456

IPv4 vs. IPv6 Headers

IPv4 Header

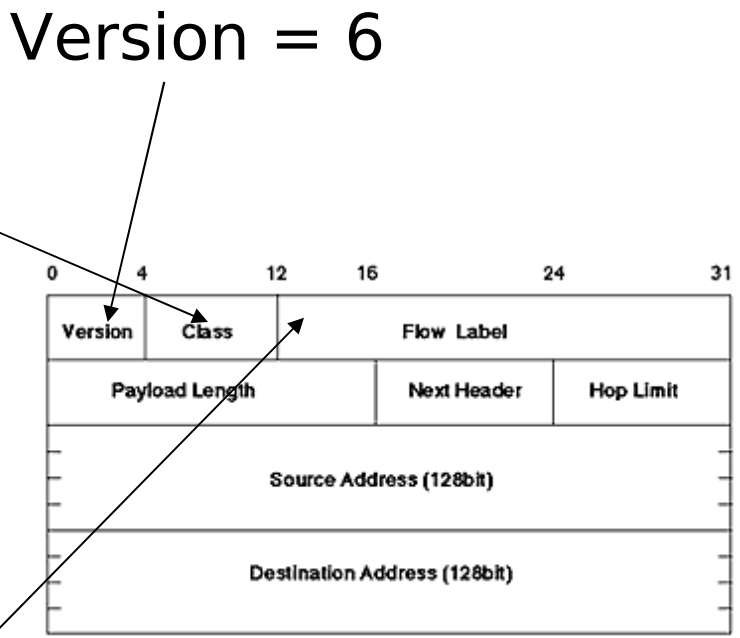


IPv6 Header

Header Attributes

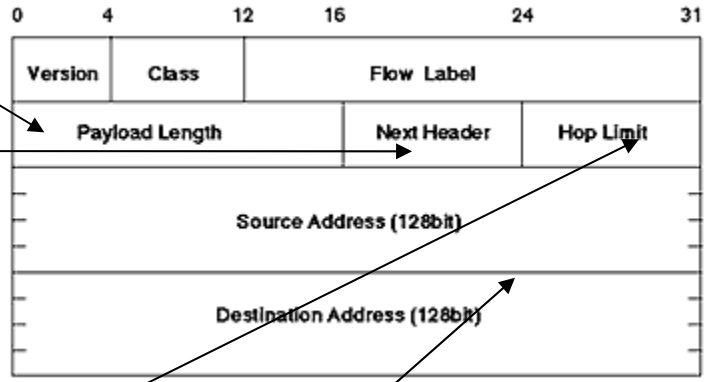
- **Traffic Class** - packet priority (8-bits). Priority values subdivide traffic, source provides congestion control and non-congestion control traffic

- **Flow label** - QoS management (20 bits)
  - Originally created for giving real-time applications special service, but currently unused



Header Attributes

- **Payload Length** - length in bytes (16 bits)
  When cleared to zero, the option is a "Jumbo payload"
- **Next header** - Specifies the next encapsulated protocol
  - TCP or UDP, plus indicates extra headers following the IP header, for options
- **Hop Limit** - replaces the time to live field IPv4 (8 bits)
- Source and destination addresses - 128 bits each



Header Changes from IPv4

- No checksum
  - Why checksum just the IP header?
    - Useful when corruption frequent, but slows processing
    - Today, corruption rare
- Different options handling
  - **IPv4 options:** Variable length header field. 32 different options! Rarely used!!
    - Many hosts/routers do not support
    - Still must compute header length, slows processing
  - **IPv6 options:** "Next header" pointer
    - Extensions headers are chained together
- No Fragmentation Built-in
  - IPv6 routers do not perform fragmentation
  - IPv6 hosts are required to either perform PMTU discovery, perform end-to-end fragmentation,
  - Or, send packets smaller than the IPv6 minimum maximum packet size

IPv6 Has Jumbograms

- IPv4 limits packets to **64 KB** of payload
- IPv6 has optional support for packets over this limit, referred to as jumbograms, which can be as large as **4 GB**
- The use of jumbograms may improve performance over high-MTU networks
- They are optionally supported by many Ipv6 devices

IPv6 Address Notation

- Pv6 addresses normally written as eight groups of four hexadecimal digits, where each group is separated by a colon (:)

- For example

  2001:0db8:85a3:0000:0000:8a2e:0370:7334

- To shorten writing and presentation of addresses, simplifications possible
  - Any leading zeros in a group may be omitted

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

IPv6 Different Addressing Modes

Unicast

- IPv4, unicast transmission data meant for single destination address only

Anycast

- IPv6 defines new type of address and transmission, known as anycast
- Anycast address is IPv6 address assigned to number of different interfaces on different systems,
  - "Fuzzy" addressing
- When packet is destined for anycast address,
  - **Closest** device to sender processes packet
    - **Closest** defined by routing protocols

Ipv6 Anycast

- Benefits
  - Anycast packet routed to "nearest" interface having that address, depending on distance along routing path
  - Service Abstraction
    - Anycast addresses can be used as service identifiers. Many services such as Domain Name System (DNS) and HTTP proxy could be accessed with anycast addressing
  - Reliability
  - Anycast address mechanism can be used for improved reliability of services
    - Anycast address can be assigned to servers scattered over Internet, a servers fails, other servers can still provide service

IPv6 Different Addressing Modes

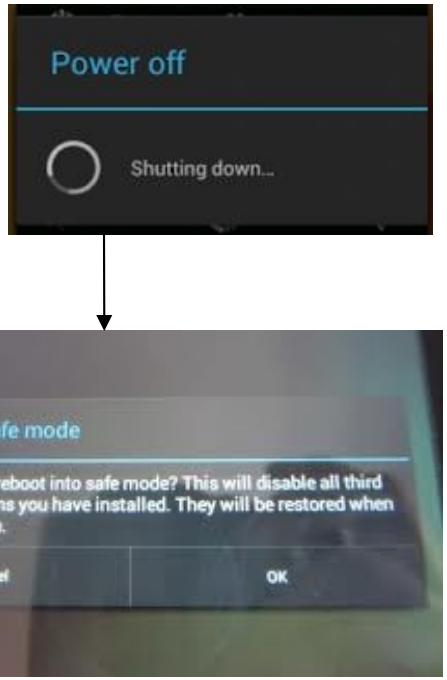
IPv6 Multicast

- If you recall, multicast transmission -> a single transmission received by many systems,
- Or a one-to-many technique
- **In IPv6**, multicasts more flexible
- Prefix FF00::/8 with several options
  - Examples of multicast addresses used in IPv6 include destination address FF02::1, used to send a multicast to **all hosts** on a given subnet
  - Similarly, multicast address FF02::2, used to communicate with **all routers** on a subnet

Migrating from IPv4 to IPv6

- How would you do it?
- Idea is to still maintain Ipv4 space but gradually migrate to IPv6

Migrating from IPv4 to IPv6

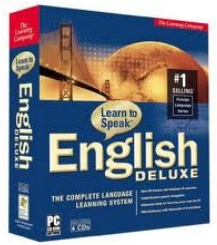


- How do you upgrade the Internet?
- **Instigate migration mechanisms**
  1. Dual-Stack
  2. Manual Configured Tunneling
     IPv6 traffic through IPv4 networks
  3. Automatic tunnels “6to4” Connection of IPv6 Domains
     via IPv4 Clouds,

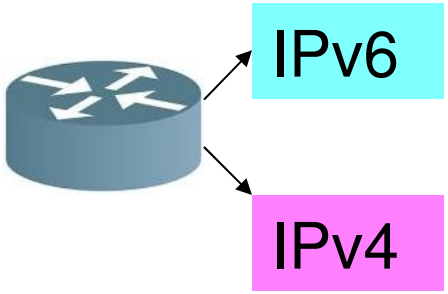
     Other methods too ...

IPv6 Dual Stack

- One technique, called **dual stack**, involves running **IPv4 and IPv6** at same time
  - Think of speaking both French and English but not at the same time!
- End nodes and routers/switches run both protocols
  - IPv6 communication is possible, that's preferred protocol
- For hosts, this means that host has both an IPv4 and IPv6 address associated with each NIC
  - Host can send **IPv4** packets to other **IPv4** hosts
  - Host can send **IPv6** packets to other **IPv6** hosts

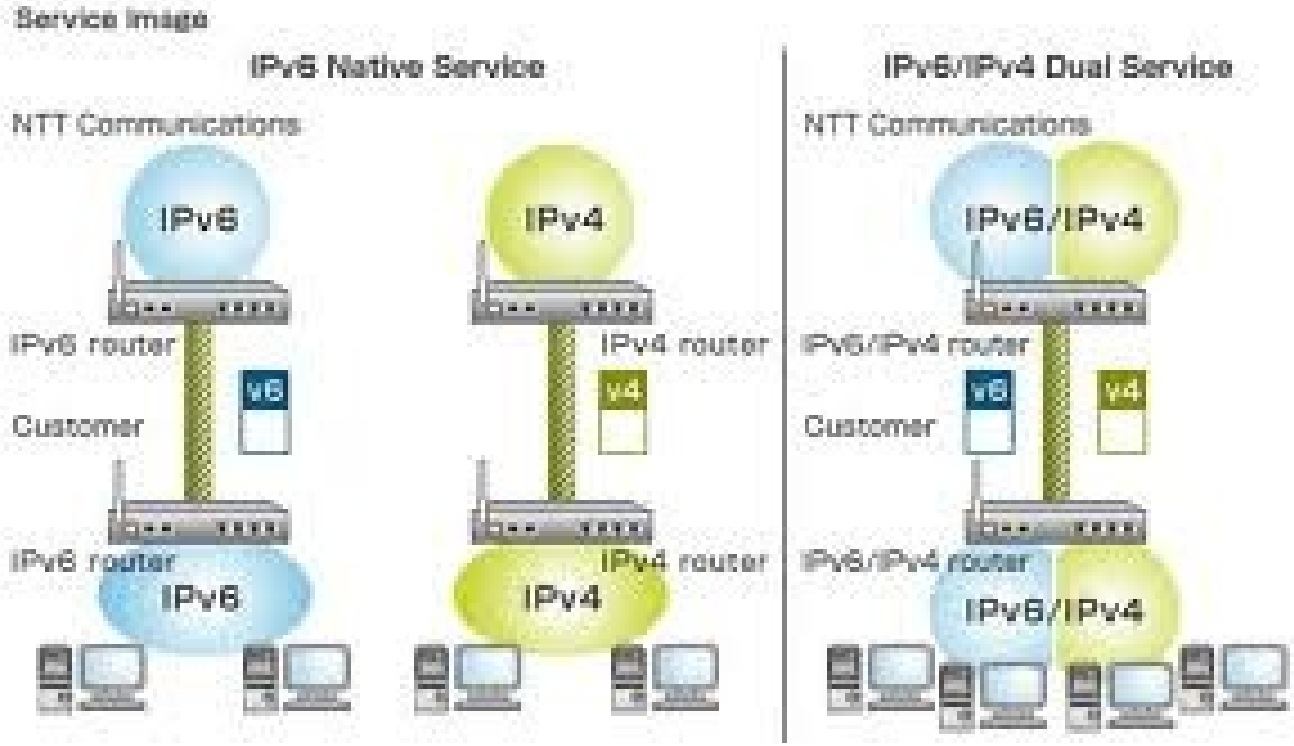


IPv6 Dual Stack



- For routers, it means that
  - In addition to the usual IPv4 IP addresses and routing protocols, routers would also have IPv6 addresses and routing protocols
- To support both IPv4 and IPv6 hosts,
  - Router could then receive and forward both IPv4 packets and IPv6 packets

Dual Ipv6 and Ipv4 Service



Tunneling in General

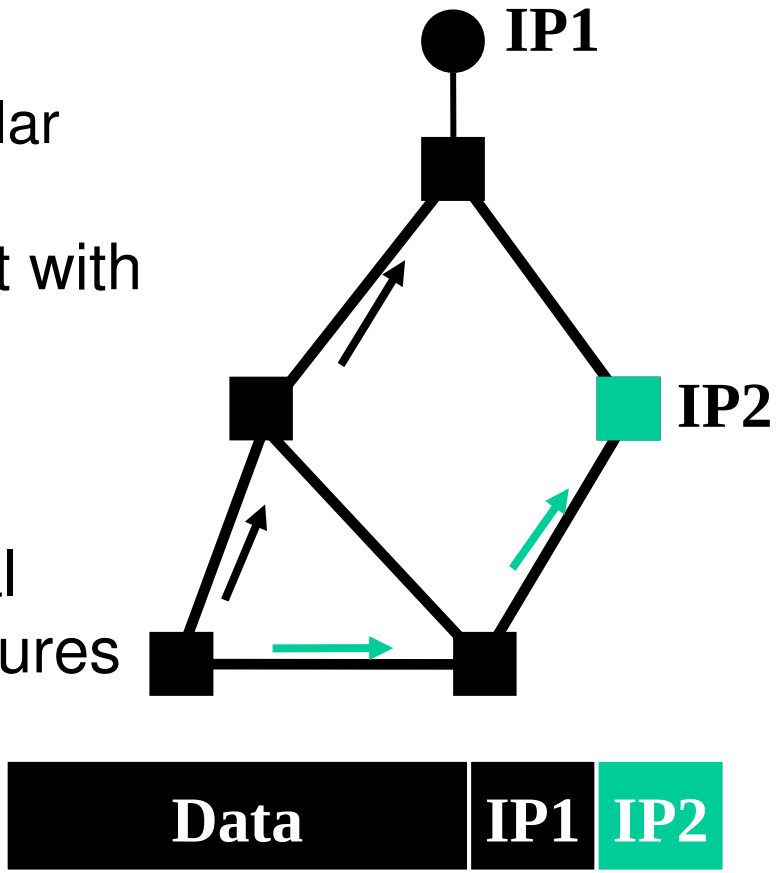
- Tunnel Ipv6 traffic over the Ipv4 protocol
- What is tunneling?

Concept of Tunneling

Force a **packet** to go to a specific point in the network

- Path taken is different from regular routing

- Add an extra IP header to packet with a new destination address
  - Like putting a letter in another envelope
- Increasingly used to deal special routing requirements or new features
  - Mobile IP,..
  - Multicast,
  - IPv6 …



Tunnel Details

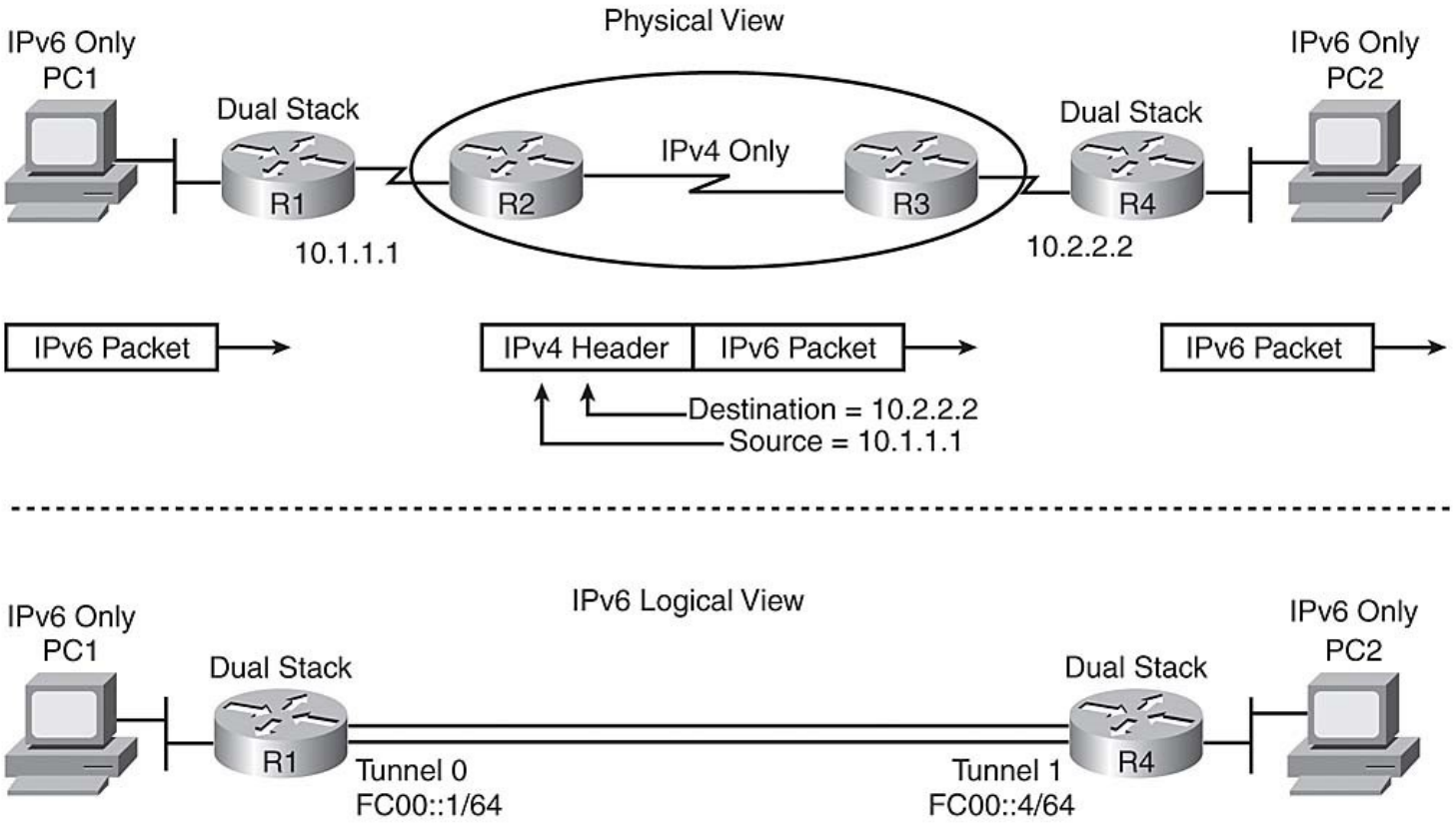
- IP **source** and **destination** address identify tunnel endpoints
- Inner header is not modified, except for decrementing TTL
- Example of Ipv6 over Ipv4

Manual Configured Tunnel

- Manually configured tunnel is permanent virtual link between two IPv6 networks connecting over an IPv4 backbone
- Routers at source and destination of tunnel must have IPv4 and IPv6 dual stack protocols
- Because these tunnels have to be configured manually they are not very scalable
- So this type of tunnelling is for permanent links

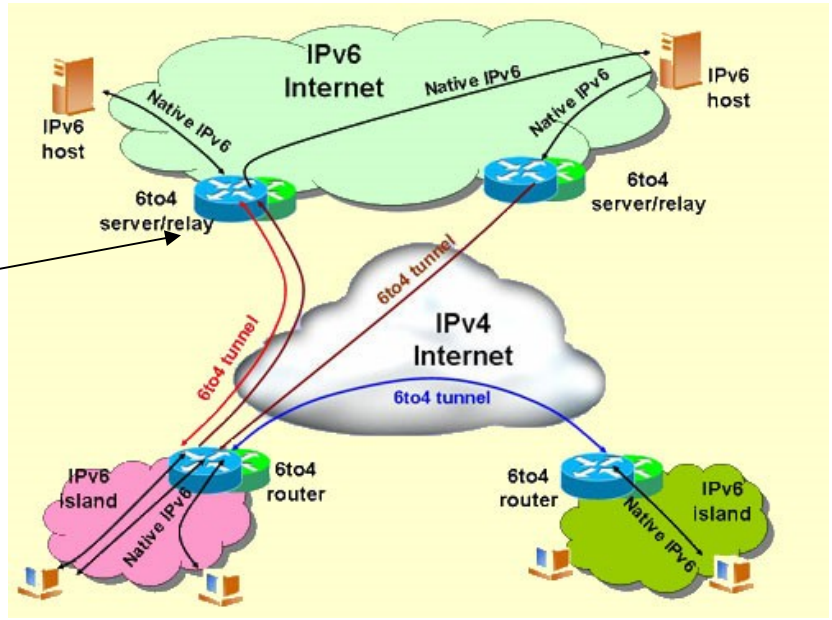
IPv6 Tunneling in General

- The concept is very much like a VPN tunnel



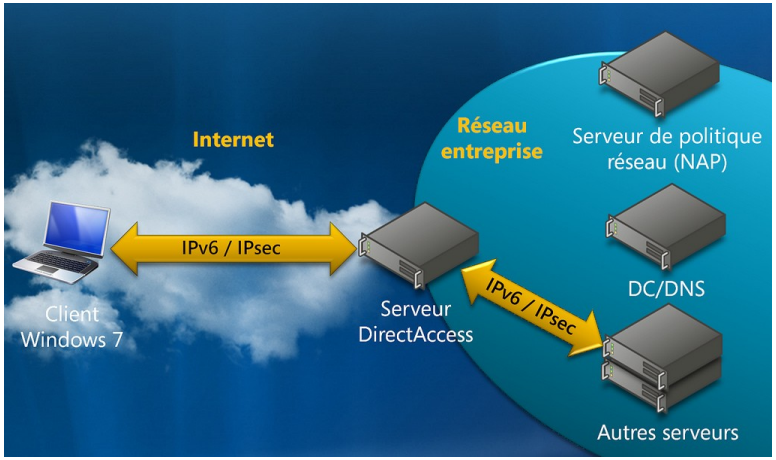
IPv6 6to4

- 6to4 (sometimes written 6 to 4), system allows IPv6 packets to be transmitted over an IPv4 network **automatically**, without need to configure explicit tunnels
  - Routing conventions are also in place that allow 6to4 hosts to communicate with hosts on the IPv6 internet
  - 6to4 Relay routers



IPv6 6to4

- 6to4 uses a special IPv6 prefix
  - 2002::/16. IANA has set aside this address space just for 6to4
  - The 6to4 specification states that the 32 bits after 2002::/16 are the **IPv4 address** of the gateway machine for the network in question



Ipv6 and IPSec

Argument for IPvSec in Ipv6

End-to-end security
- Kind of important
- Shopping in the Internet

  Credit card numbers, electronic money, identity of the sender, integrity of electronic bills

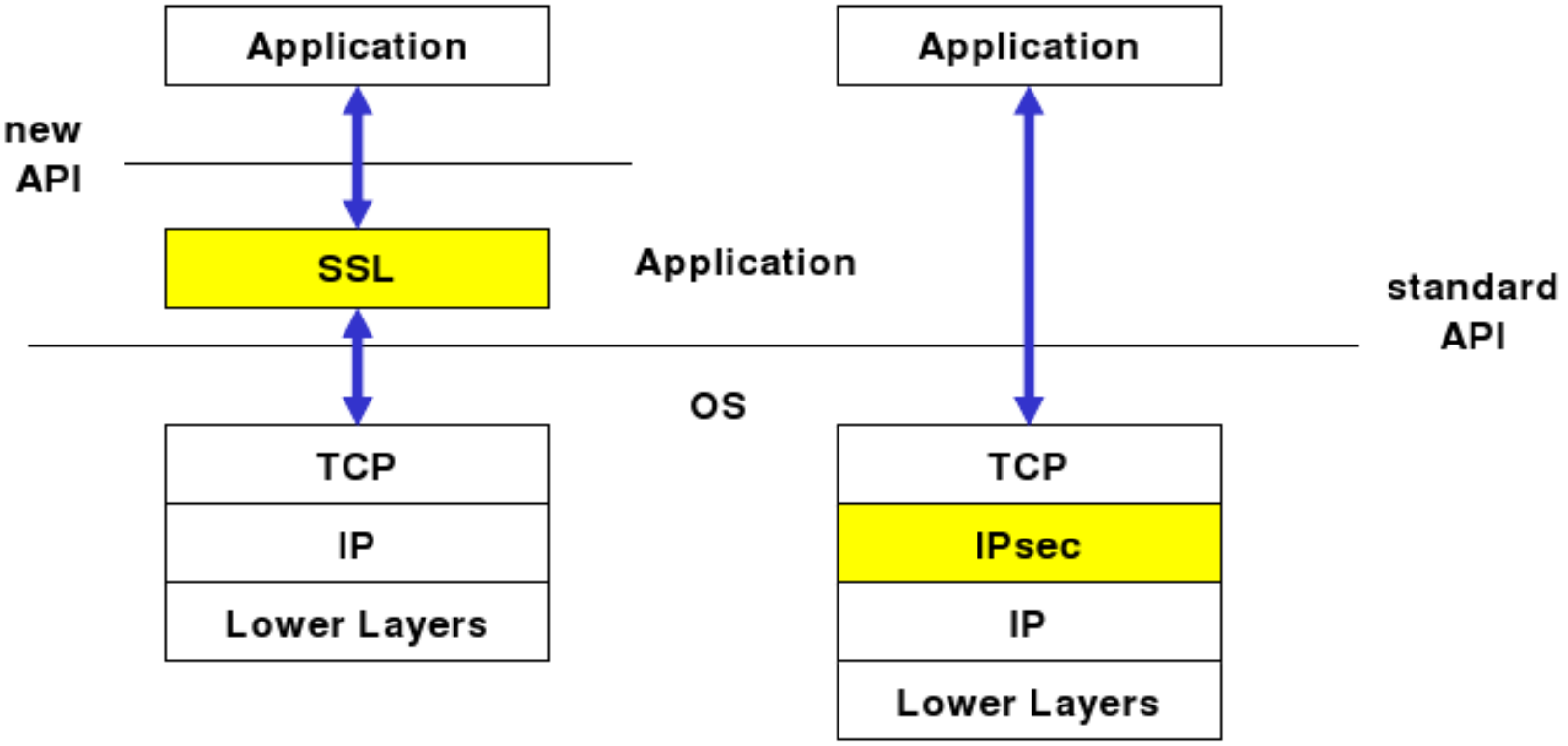
- Question was in design of IPv6
  - Should next generation IP protocol (IPv6) provide end-to-end security as integral part of itself

- What's best network layer to provide security?

Which Layer for Security?

Application must be aware of new application programming interface

Application can use standard application programming interface



Security Issues in IP

- Source spoofing
- Replay packets
- No data integrity or confidentiality

Threats

- Attacks
- DOS attacks
- Replay attacks
- Spying
- and more…

Fundamental Issue:

Networks are not (and will never be) fully secure

Goals of IPSec

1. Verify sources of IP packets
   Authentication
2. Protect integrity and/or confidentiality of packets
   Data Integrity/Data Encryption

References

Illustrated Guide to IpSec

http://www.unixwiz.net/techtips/iguide-ipsec.html

Wikipedia

http://en.wikipedia.org/wiki/IPsec

What IPsec does?

- **IPsec enables a system**
  - to select required security protocols, determine the algorithm's to use for the services, and put in place any cryptographic keys required to provide the requested services
- **IPsec can be used**
  - to protect one or more "paths" between a pair of hosts, between a pair of security gateways (VPN), or between a security gateway and a host
  - security gateway could be for example, a router or a firewall implementing IPsec
    - VPN concentrator is another name for such a device if several SA pairs are terminated at the same point
    - VPN is by far the most usual application of IPsec

What IPsec does?

- **The set of security services that IPsec can provide includes**
  - access control
    - prevents unauthorized use of a resource
    - the resource to which access is being controlled is
      - for a host -> computing cycles or data
      - for a security gateway -> network behind the gateway or bandwidth on that network
  - connectionless integrity
    - detects modification of individual IP datagram's
  - data origin authentication
  - rejection of replayed packets (optional)
    - detects arrival of duplicate IP datagram's within a constrained window
  - confidentiality (encryption)
  - all these services are provided at the IP layer
    - hence they can be used by any higher layer protocol e.g., TCP, UDP, ICMP, BGP, etc.

IPv6 and IPSec

- IPSec in IPv6 is required!!!
- IPSec in IPv4 is a separate Add-on
  - OS must be purchased with IPSec and added to devices
  - Requires OS upgrade, which is disruptive and might discourage use
- IPv6 Implementations that do not support IPSec may be considered non-compliant However ……..
- Does not mandate use of IPSec, just inclusion in protocol stack
- **IPSec turned off by default must be enabled by user**

Ipv6 References and Fun Links

The Ipv6 Forum

http://www.ipv6forum.org/

Ipv6 Information Page

http://www.ipv6.org/

Arin Information Page

https://www.arin.net/knowledge/v4-v6.html

ARIN Ipv6 Wiki

http://www.getipv6.info/index.php/Main_Page

http://www.getipv6.info/index.php/
Educating_Yourself_about_IPv6

China Ipv6

http://en.wikipedia.org/wiki/IPv6_deployment#China

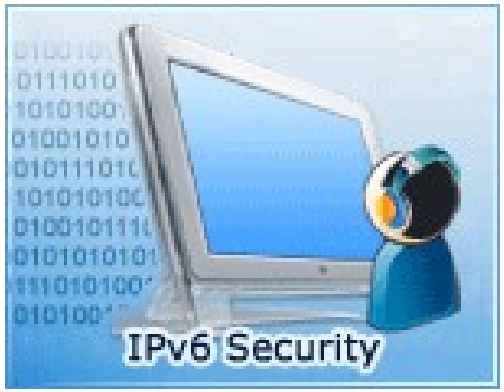
Questions for IPv6

Said … Ipv6 as a lot like Ipv4 not too many changes … but

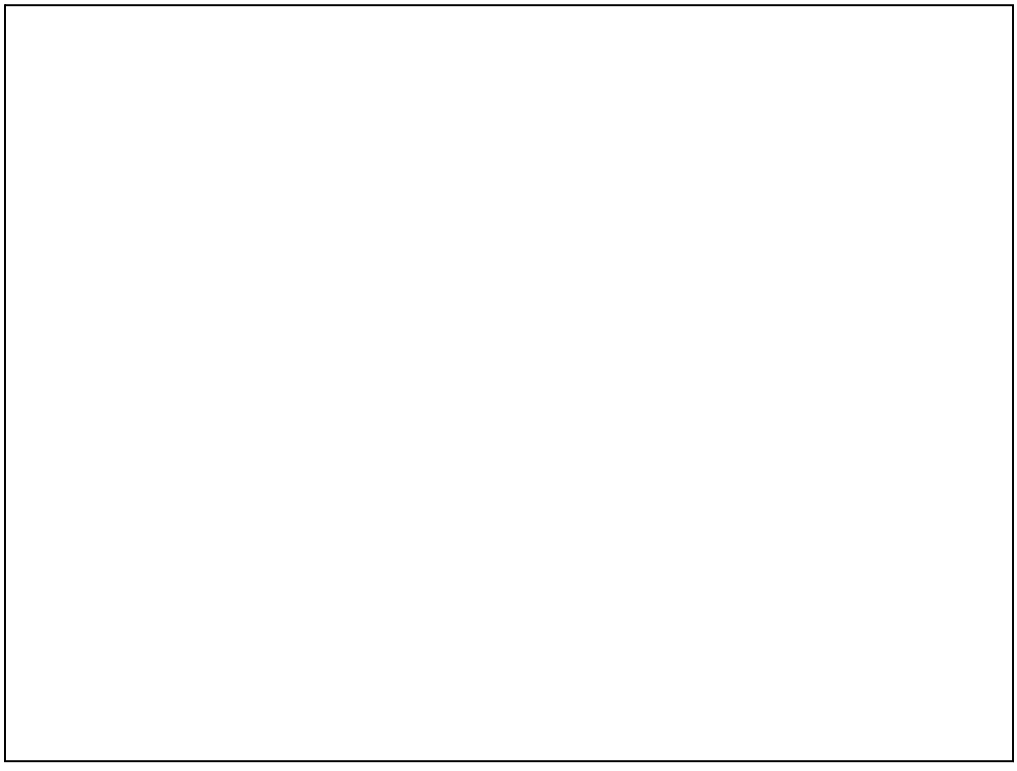
- What other protocols need to change to accommodate Ipv6?
  - Think about all the associated protocols that work with Ipv4 that facilitate addressing and routing
  - There will need to be changes to these protocols
  - ICMP6, DNS6, DHCP6, BGP

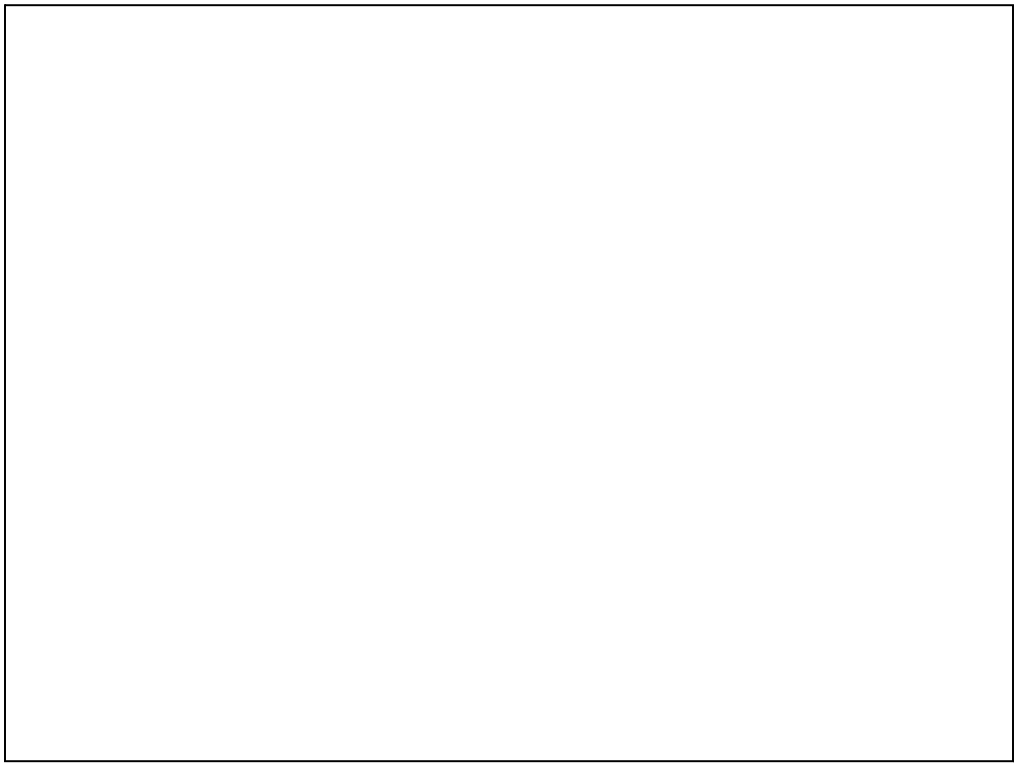
Summary

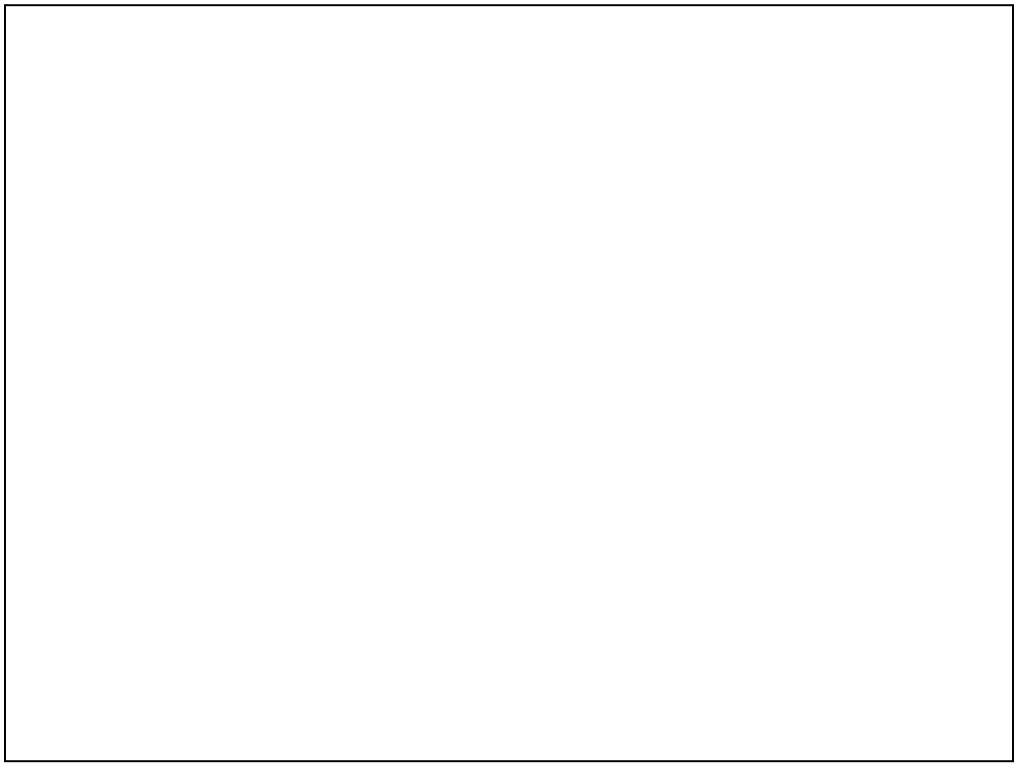
- Looked at IPv6
- It is coming, however
- As of 2011, IPv6 accounts for a small fraction of the used addresses and the traffic
- China and Europe are leading the way in adopting it
- Our government mandated all government computers will support it by 2008 … didn't really happen
- Will be interesting to see how long it does take
- Will happen in our lifetime
- IPv4 addresses have run out 2011, So what?

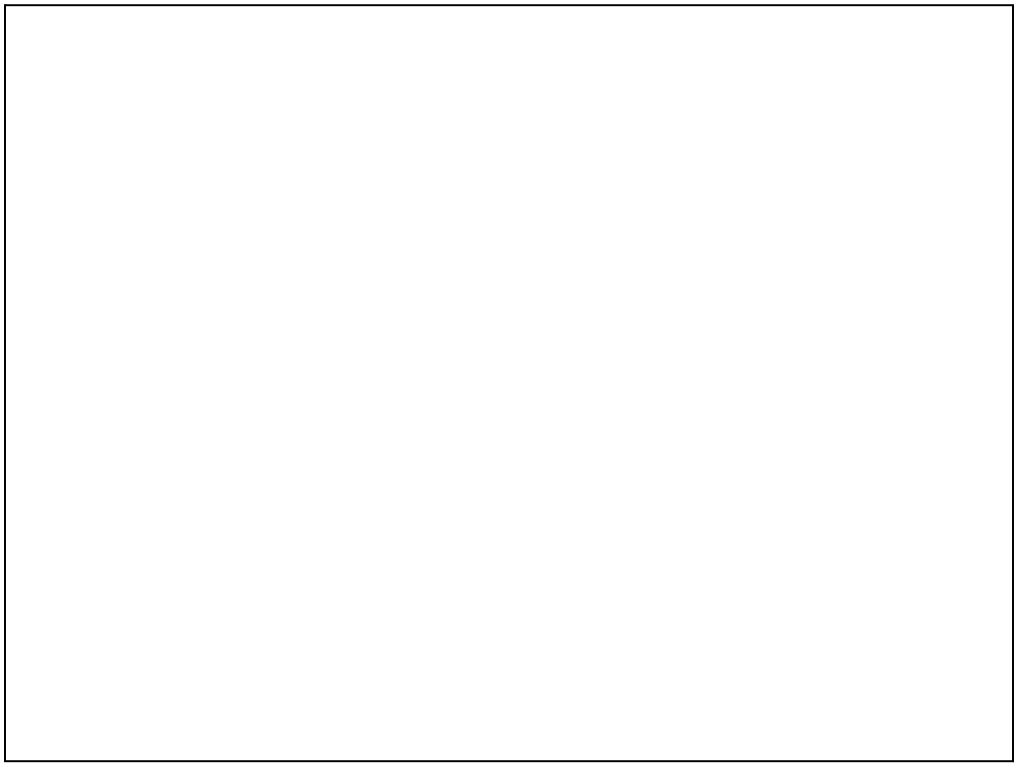


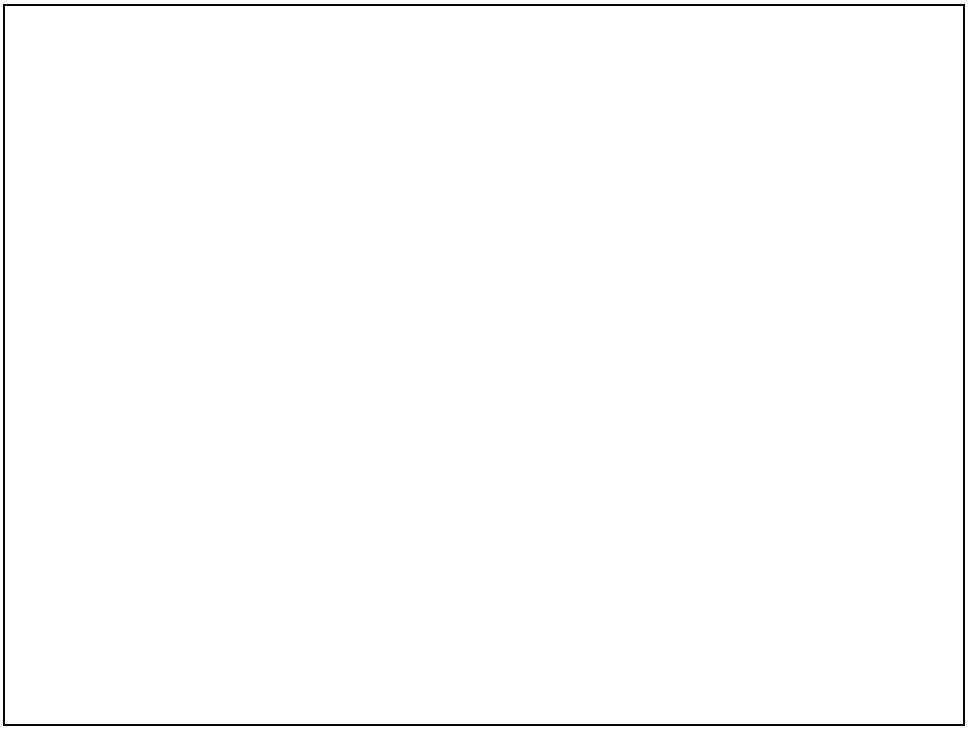
End



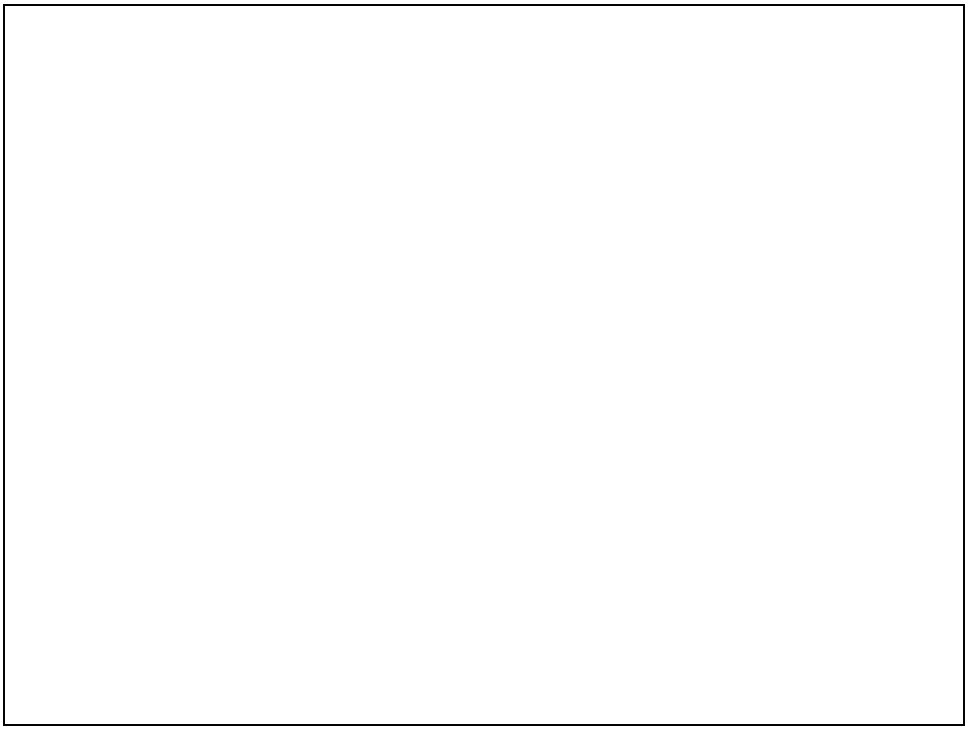








The IANA pool of IPv4 address space depleted on February 3, 2011. This slide shows the steady depletion of that pool over time.

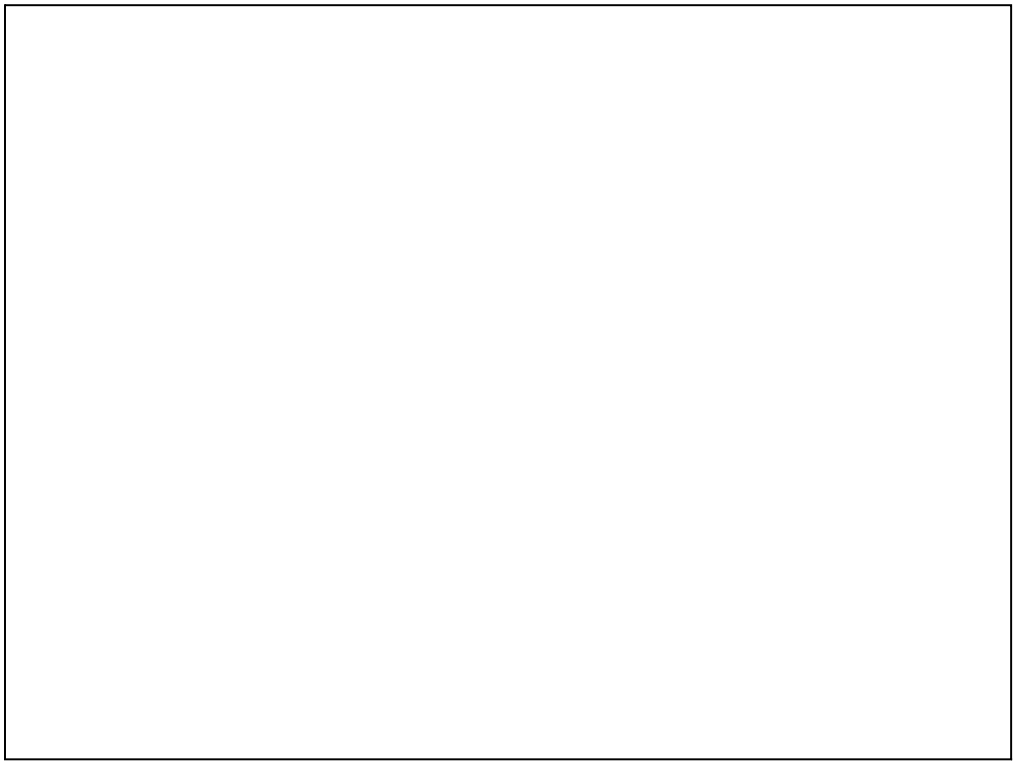


Now that the IANA IPv4 pool has depleted, the RIRs are left with their final existing inventories. Demand for the resource will determine when the RIR IPv4 pools deplete. We expect the pools to begin depleting before the end of 2011.

ICANN Feb 3 2011 Event

The IANA IPv4 Address Free Pool is now Depleted

http://www.nro.net/media-center/video-archive-3-february-2011

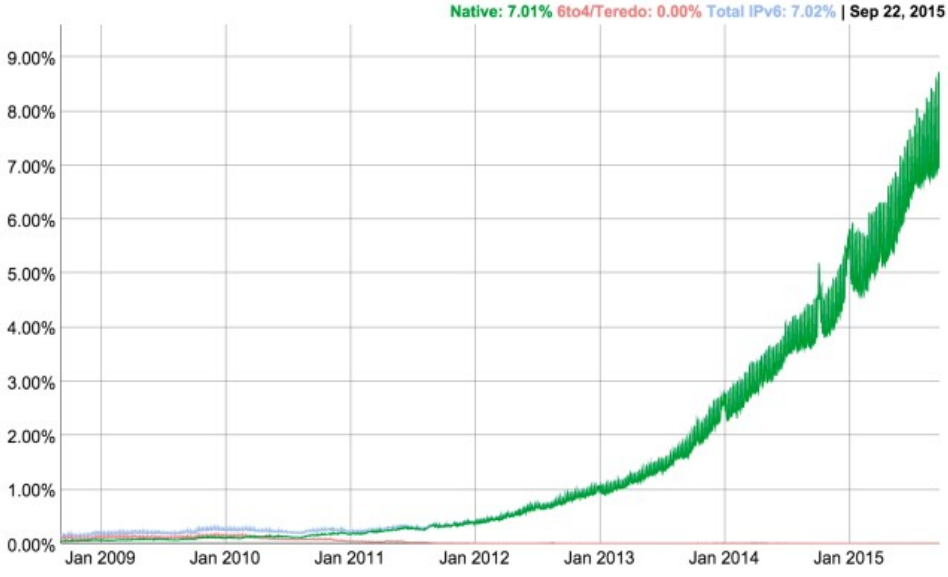


In 2016 Ipv6 Adoption

2016 is the Year of IPv6

- 10% (10.41% on January 1, to be precise) of traffic hitting Google's servers – a pretty good indicator of overall Internet traffic – is coming from an IPv6 connection
- Verizon Wireless deployed IPv6 early and both they and T-Mobile USA have large IPv6 deployments
    - Encouraging to note that four major US mobile operators now all have measurable IPv6 deployments

10 Per Cent IPv6 in 2016



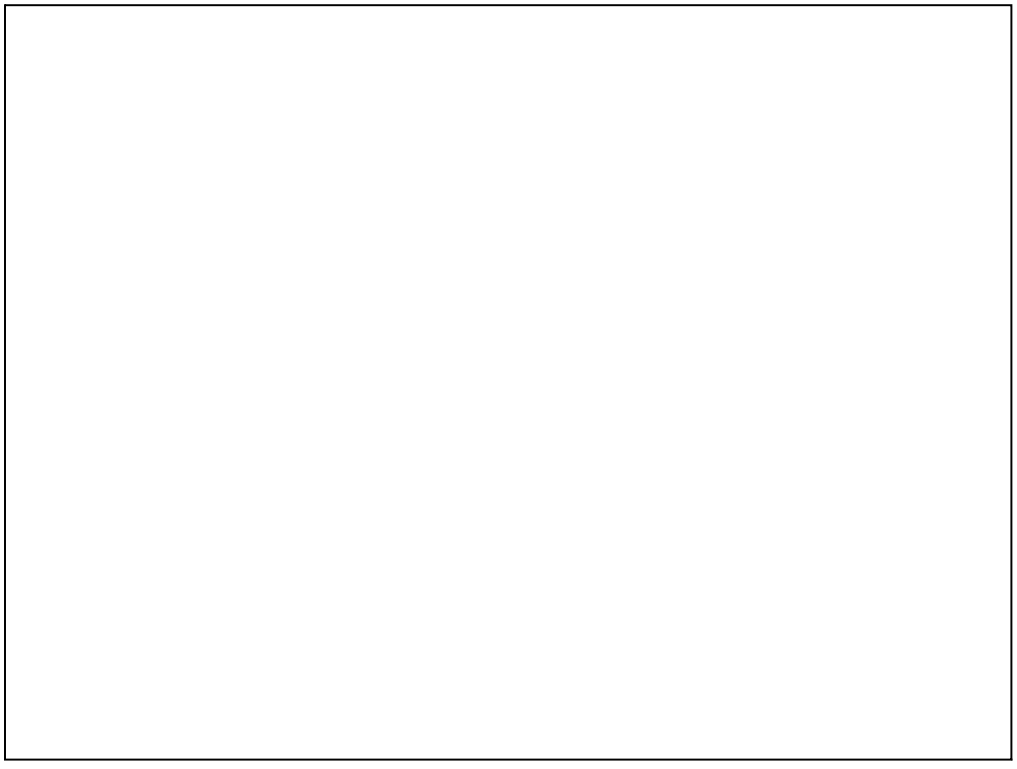
Developer Support for IPv6

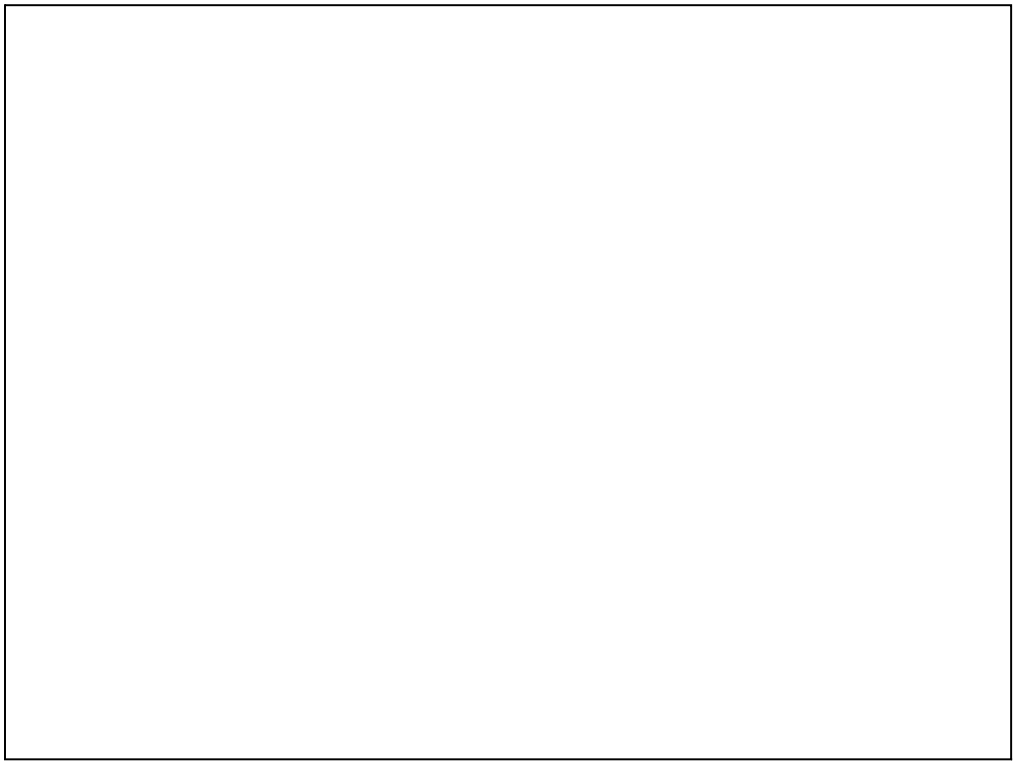
- Apple http://blogs.unity3d.com/2016/05/10/unity-and-ipv6-support/
  - At WWDC 2015, announced that iOS 9 will support IPv6-only network services
  - All apps submitted to the App Store must support IPv6 starting in early 2016

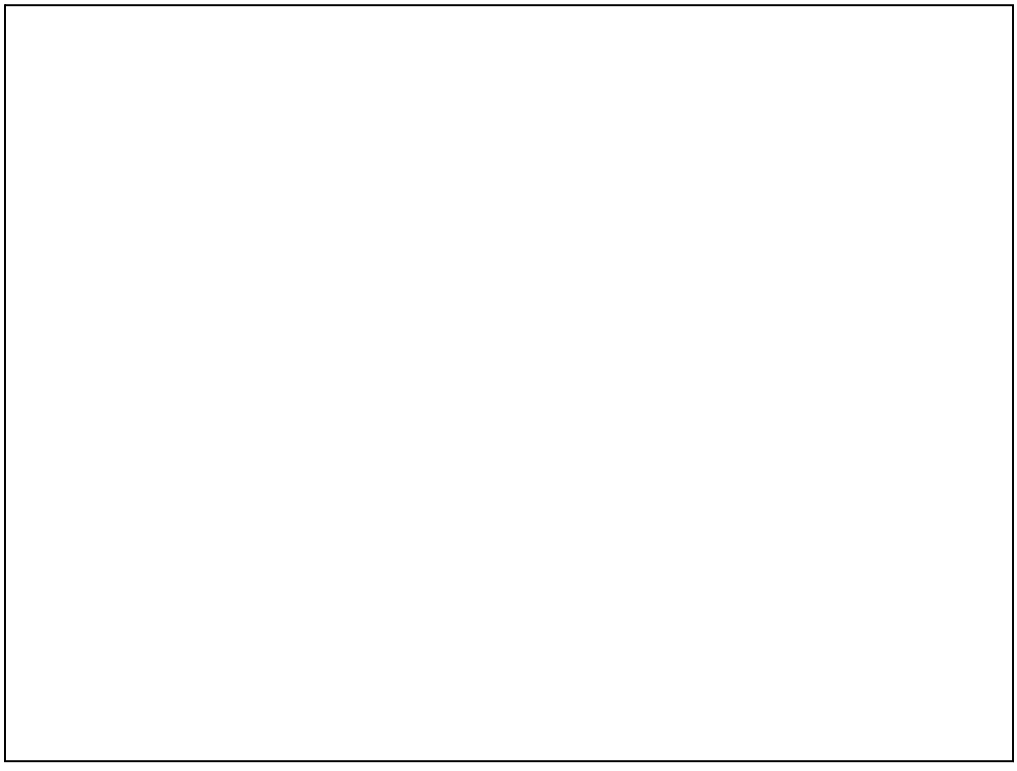
  - Microsoft

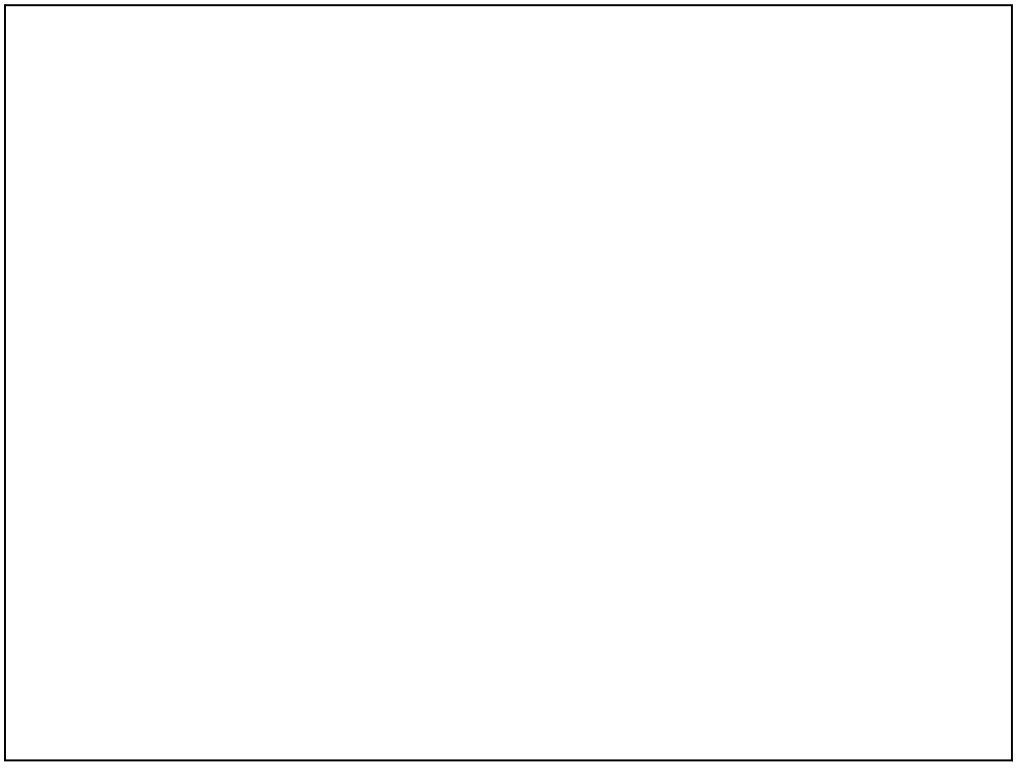
    Microsoft is not so advanced

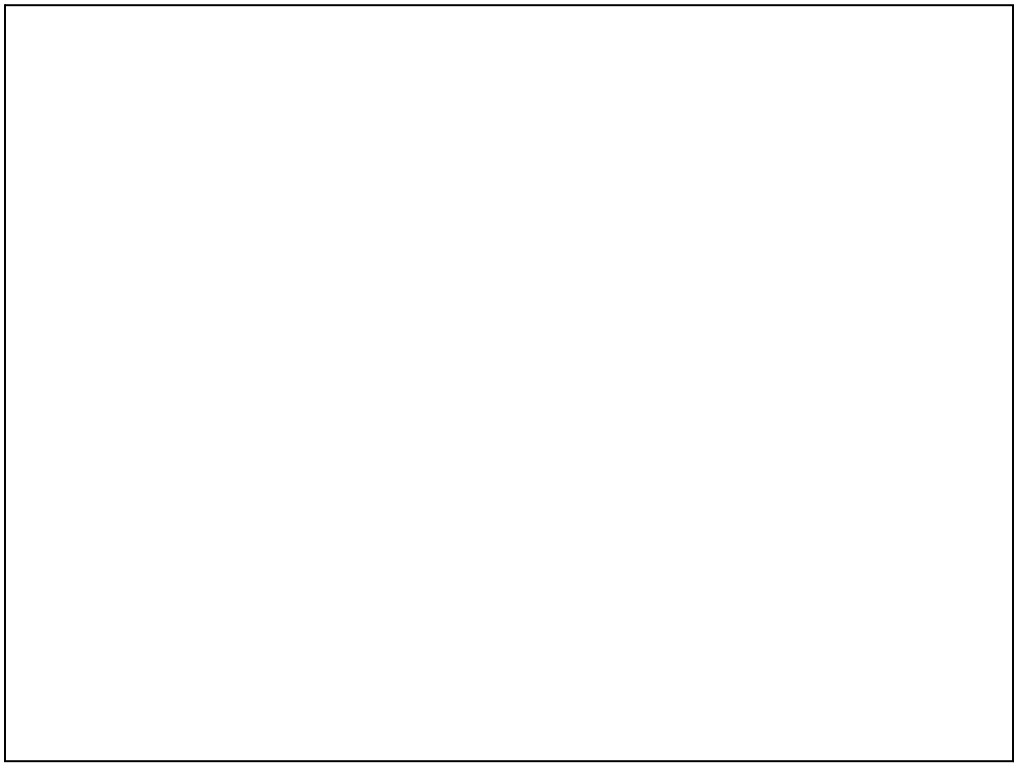
    https://technet.microsoft.com/en-us/network/hh994905.aspx

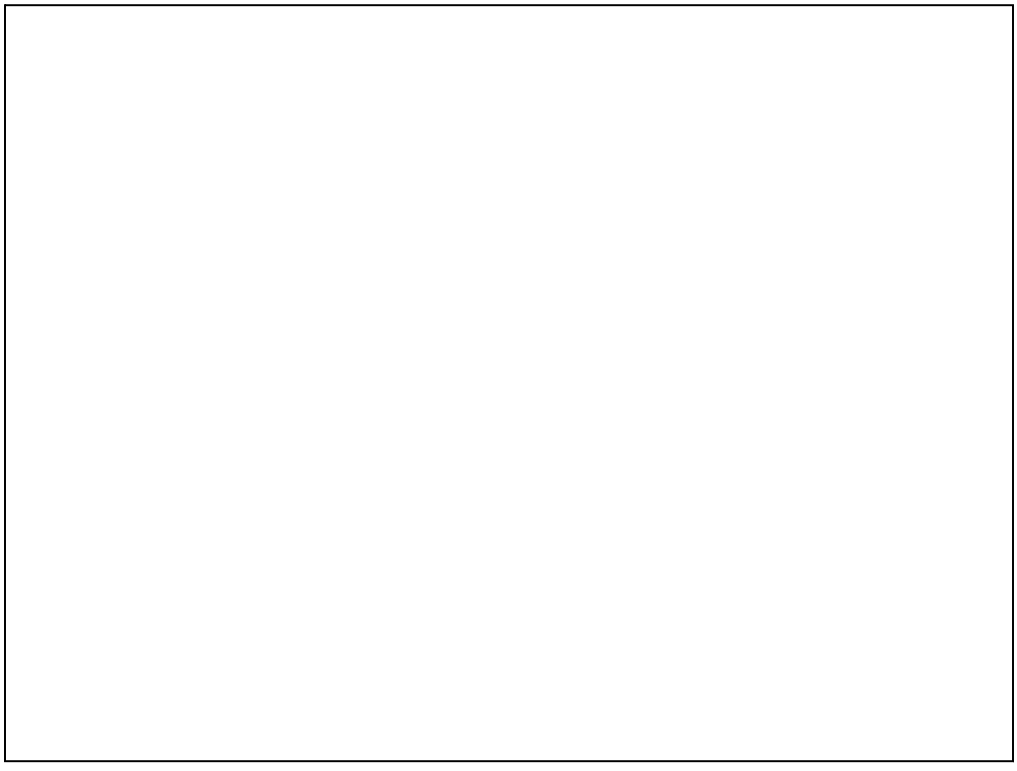


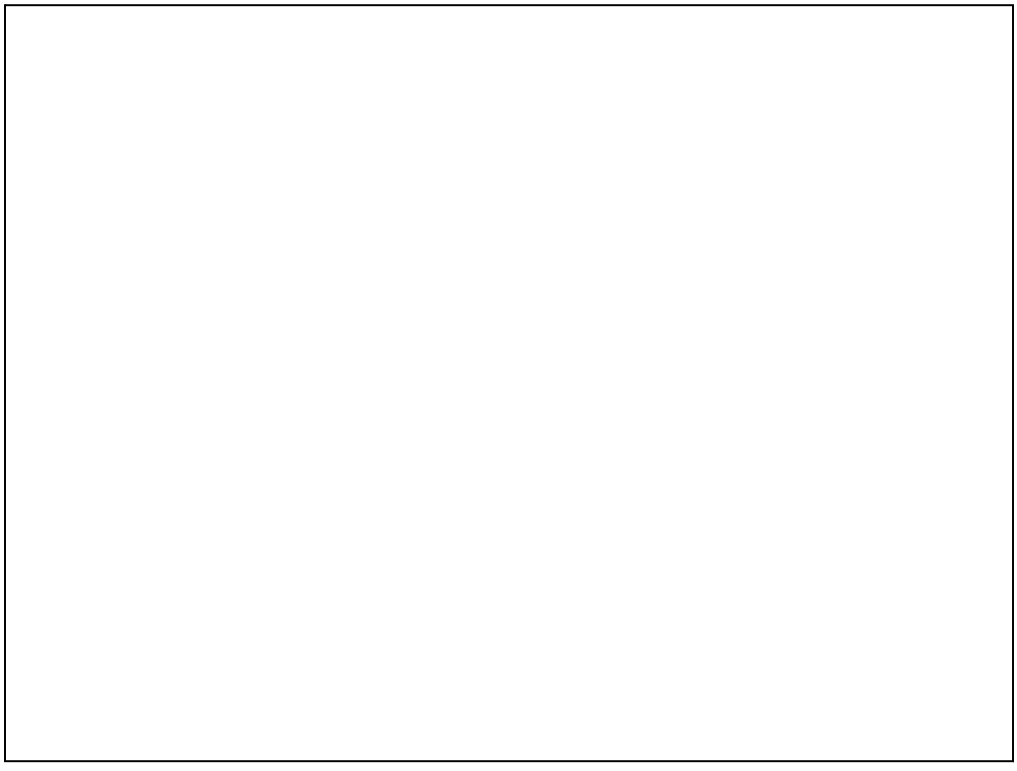


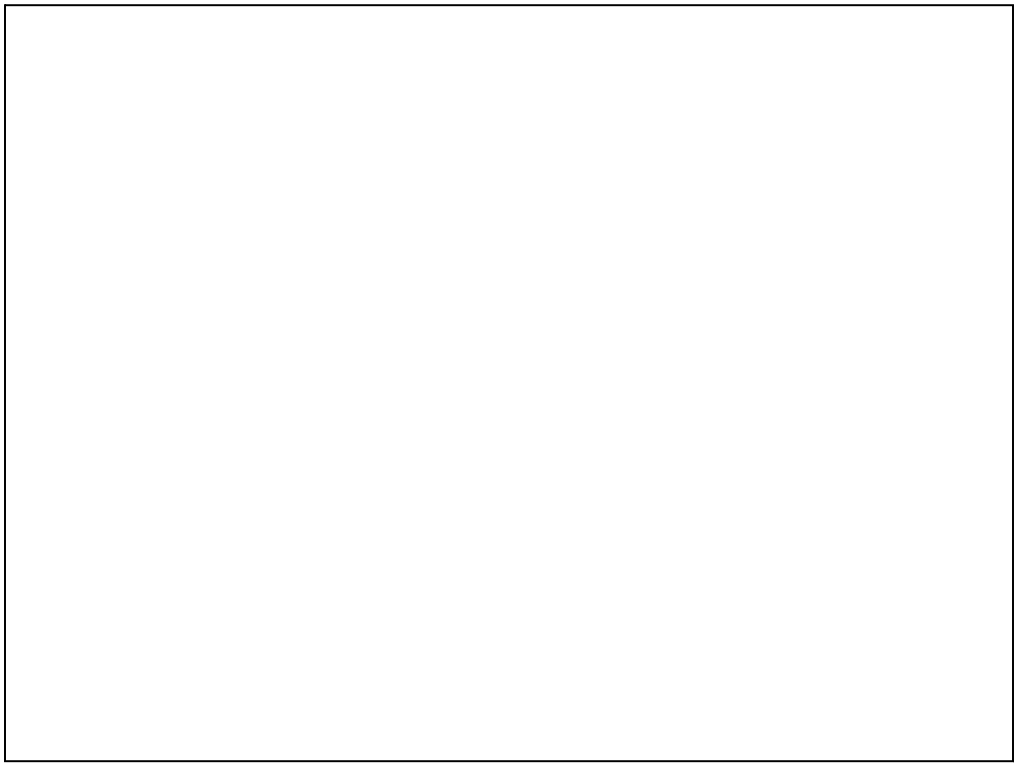




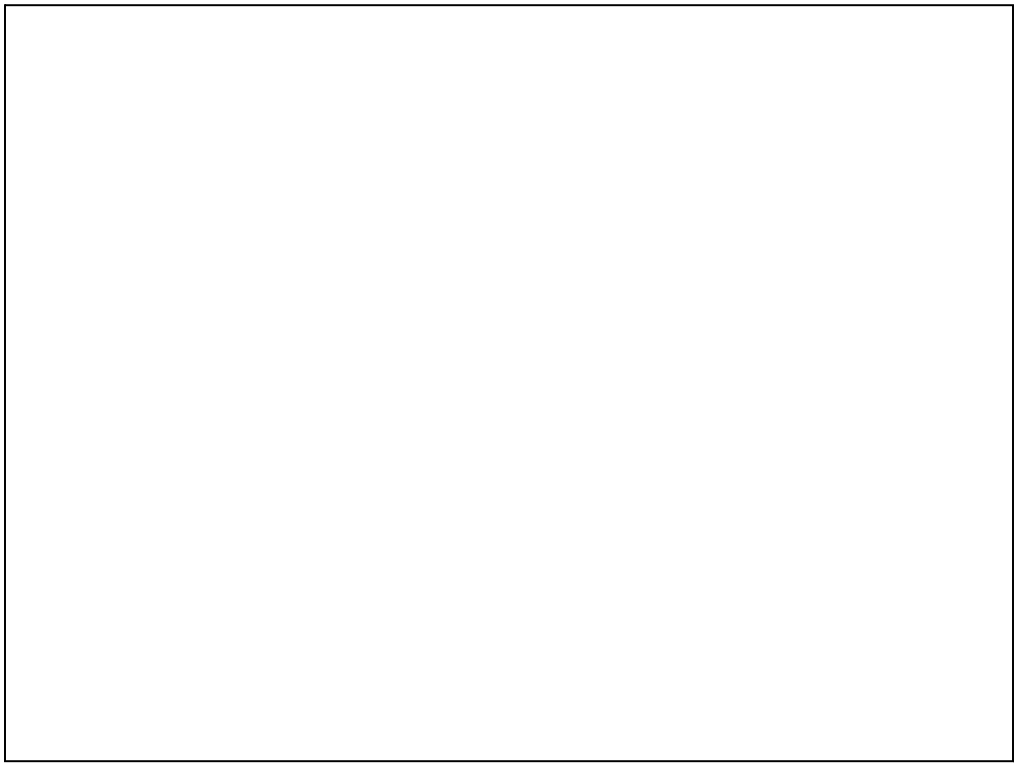


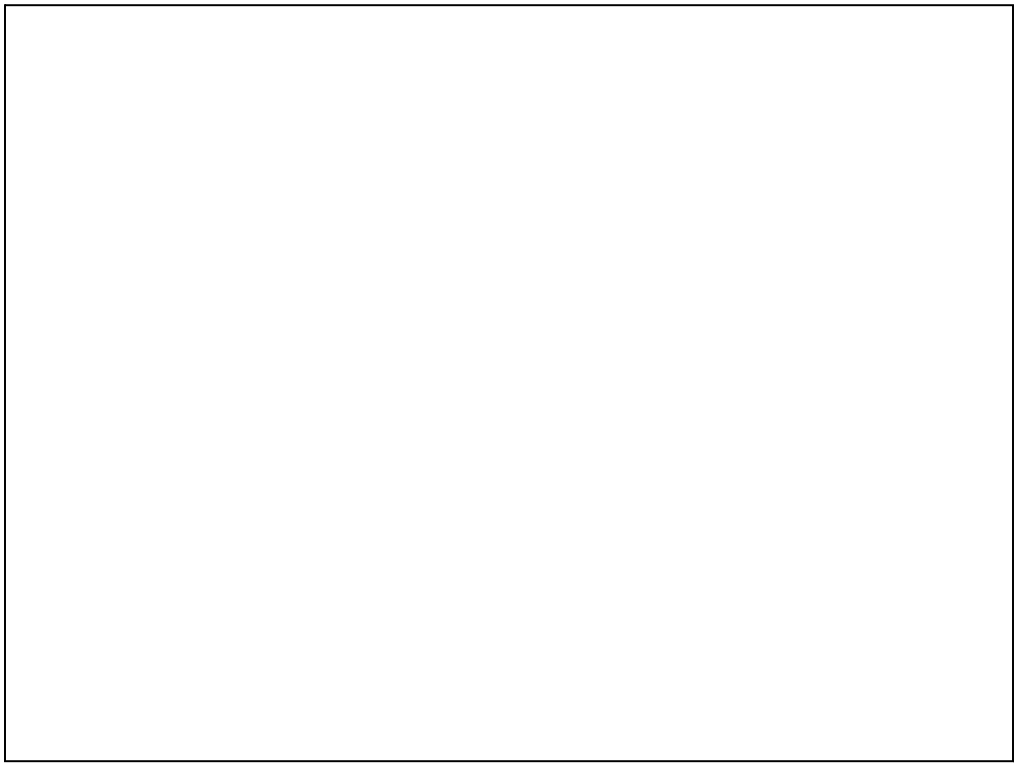


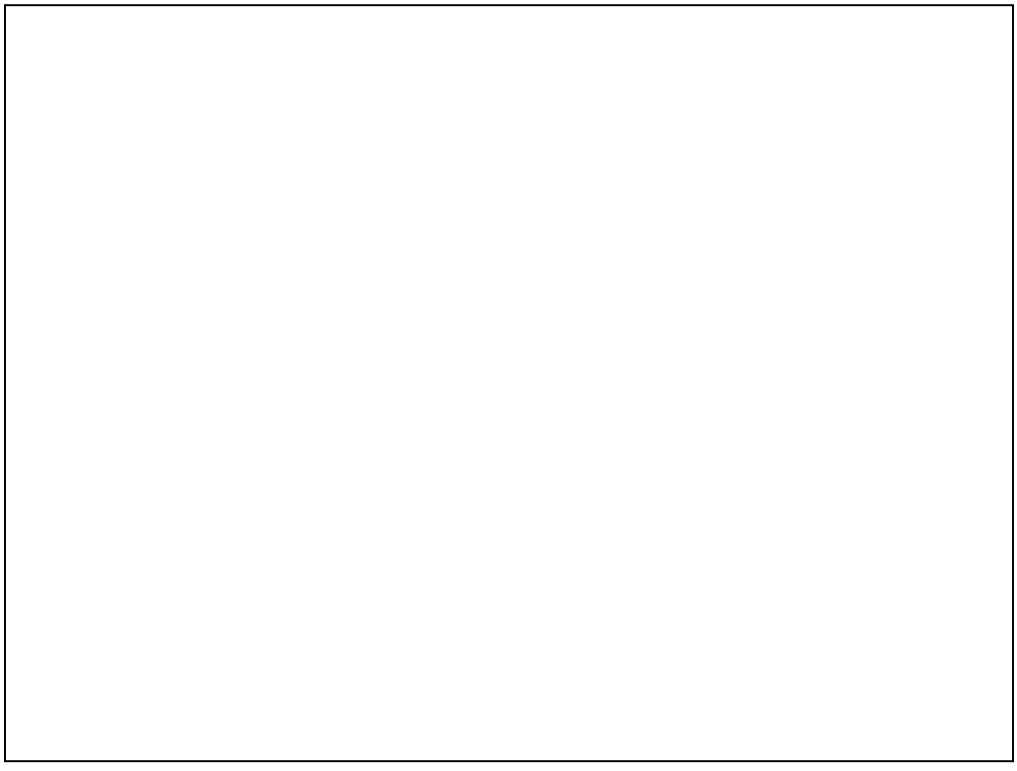


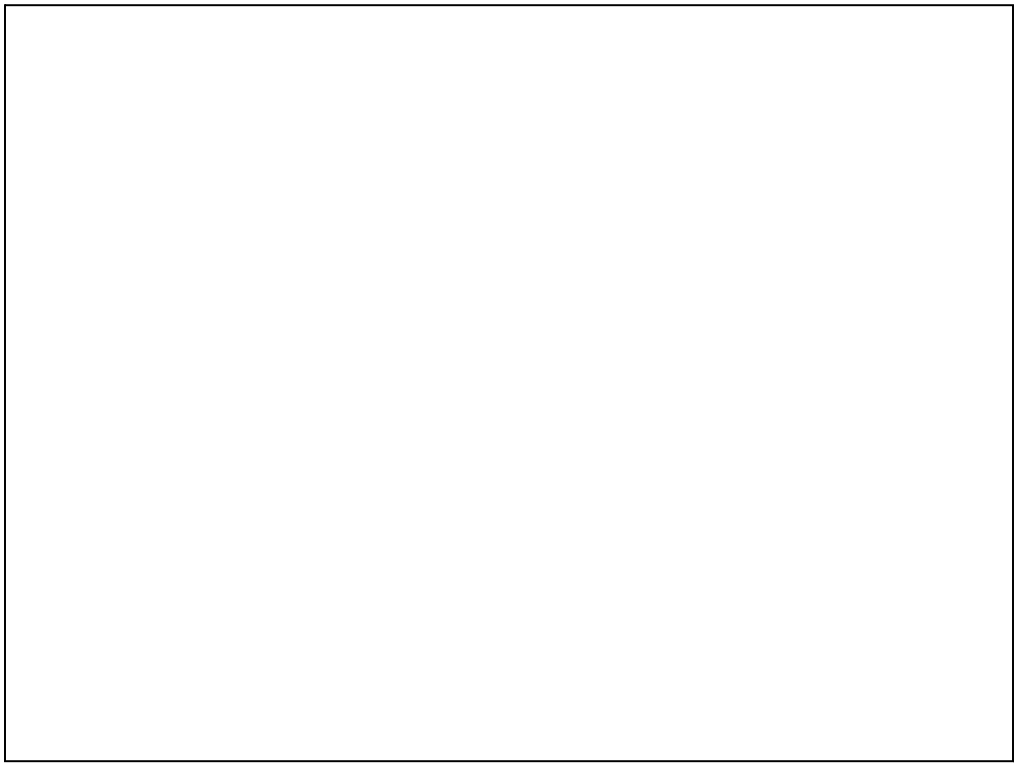


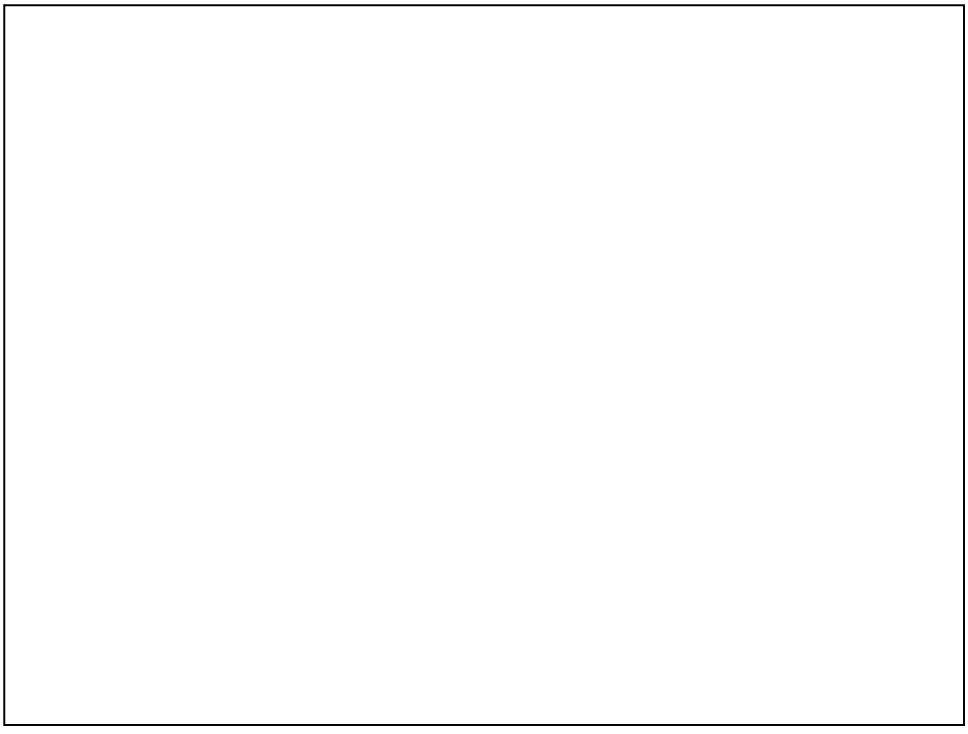
IPv6 the Next Implementation



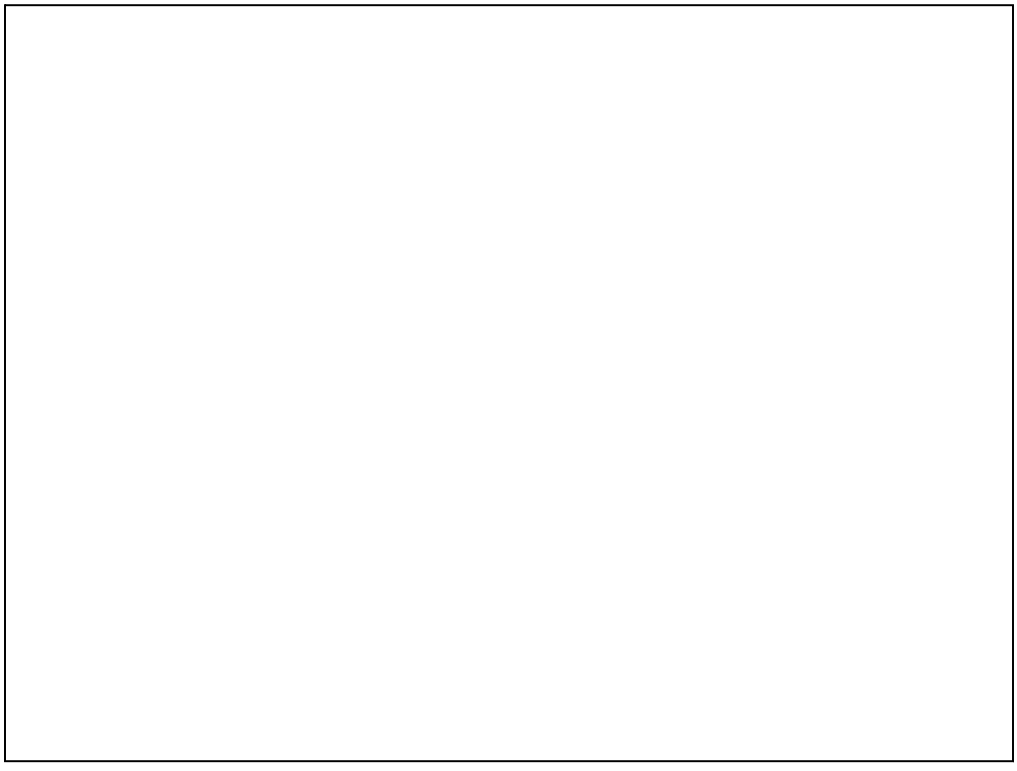


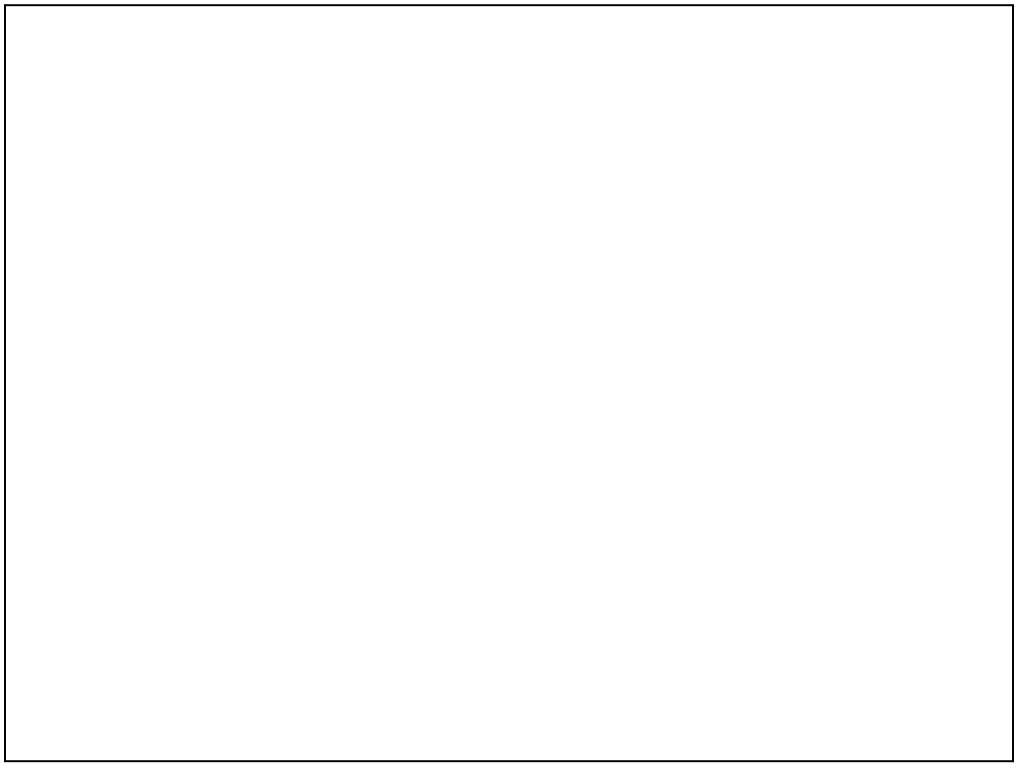


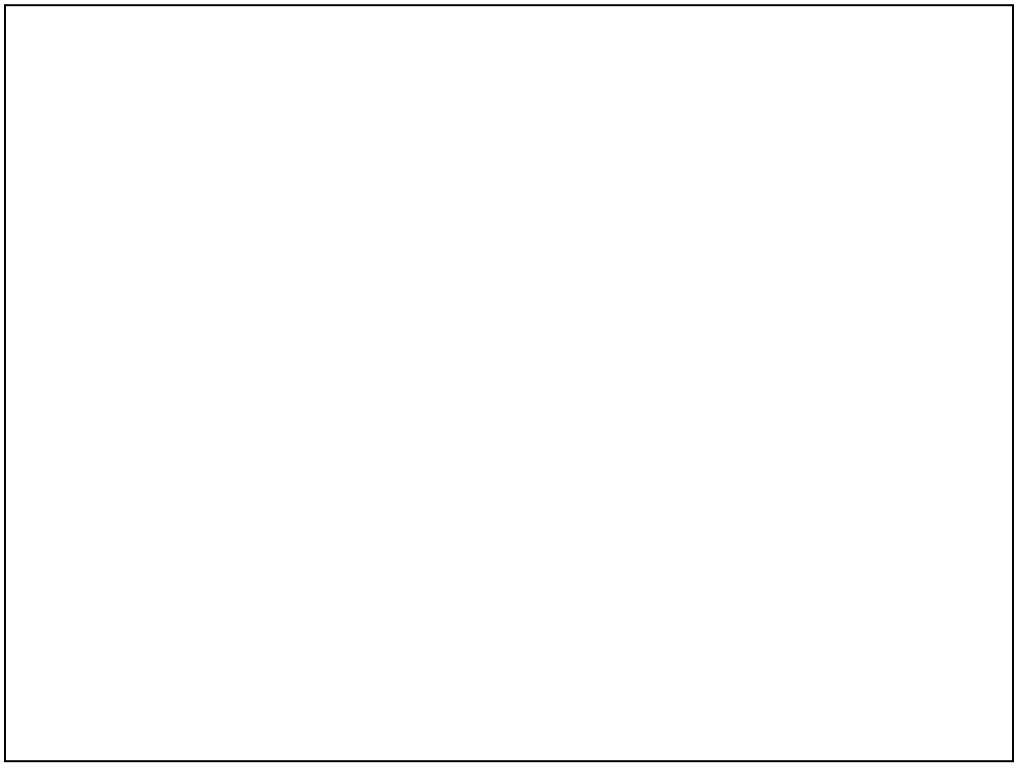


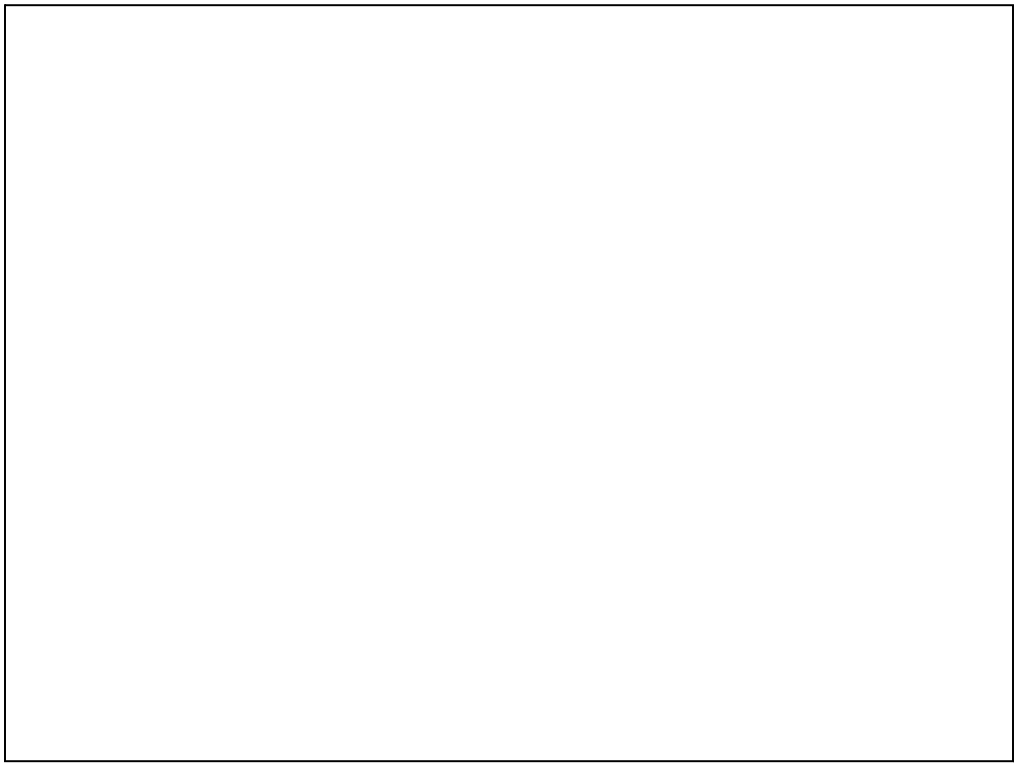


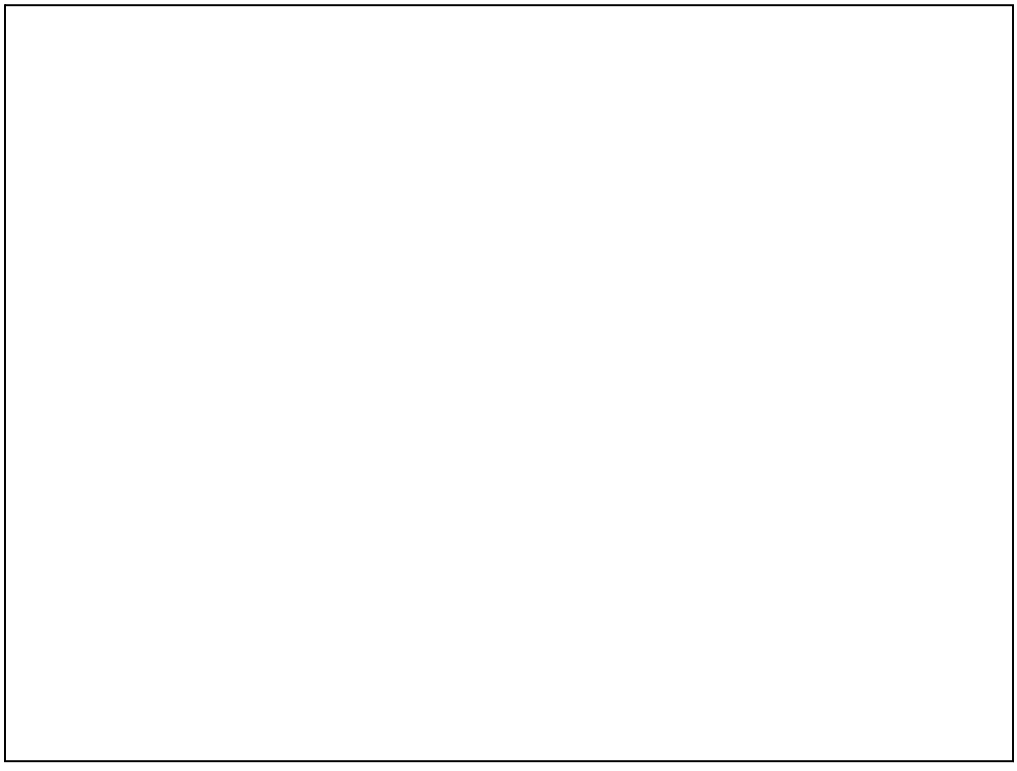
IPv4 address space has been used for decades to grow the Internet. When engineers deployed IPv4 in 1981, four billion IP addresses seemed like plenty. As the world caught on to the commercial possibilities of the Internet, though, engineers realized that the number of IP addresses simply wasn't enough for all the laptops, mobile devices, web servers, routers, and other devices coming online. The first allocation of IPv6 address space by a Regional Internet Registry (RIR) to a provider was made in April of 1999.

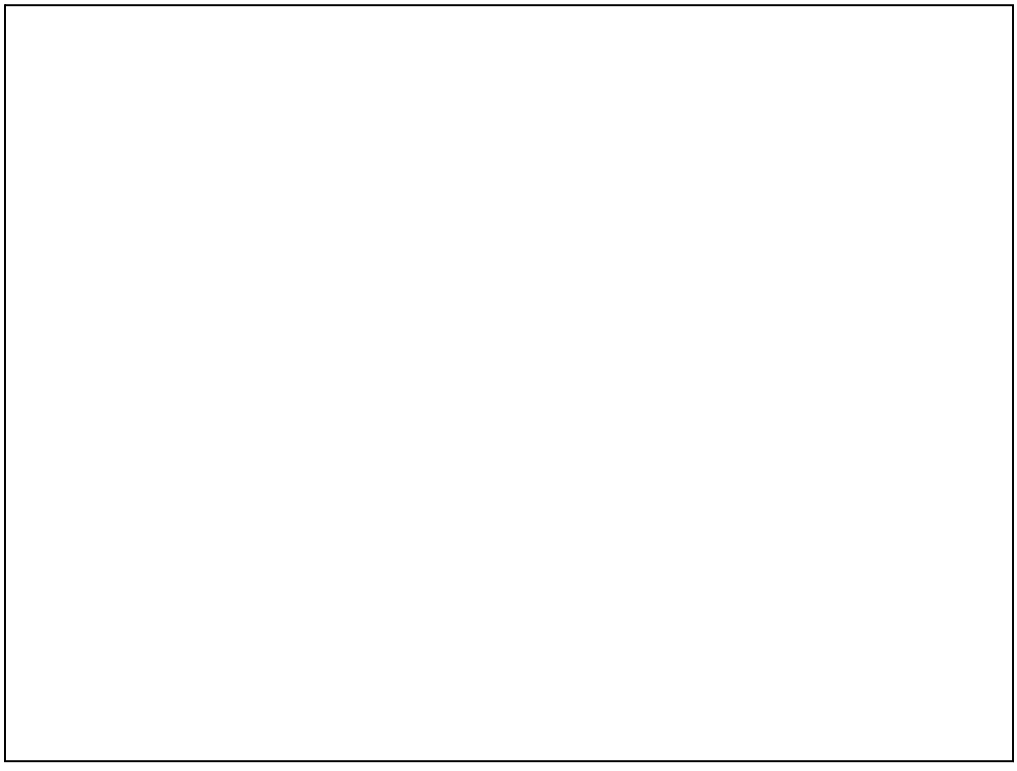


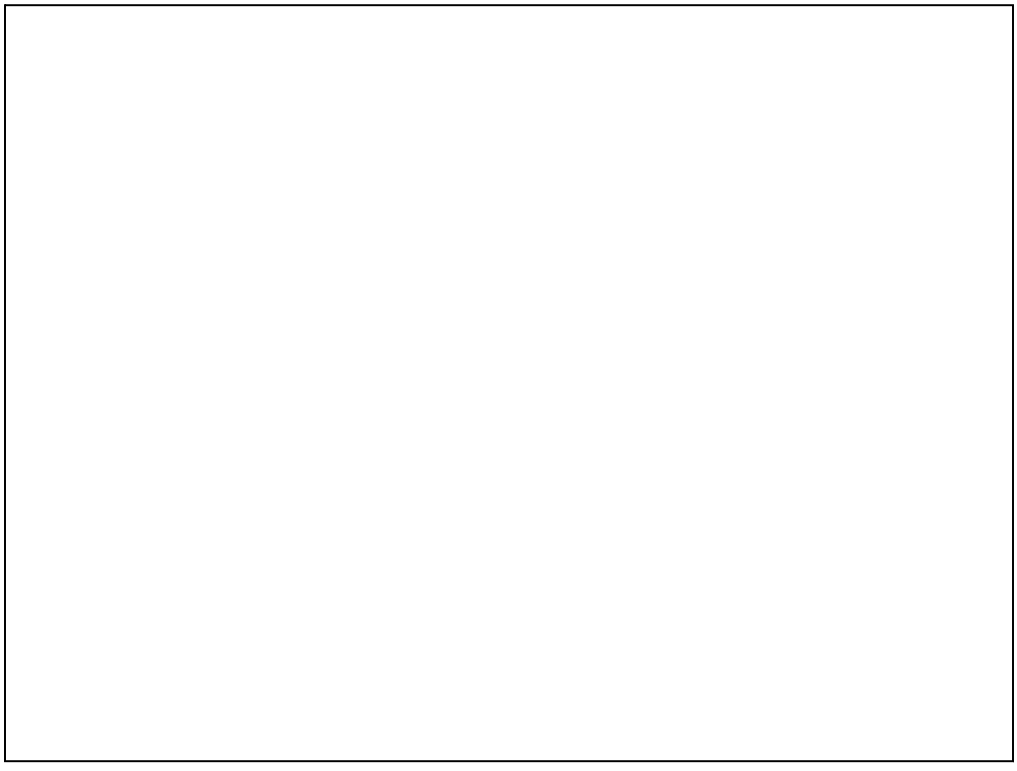






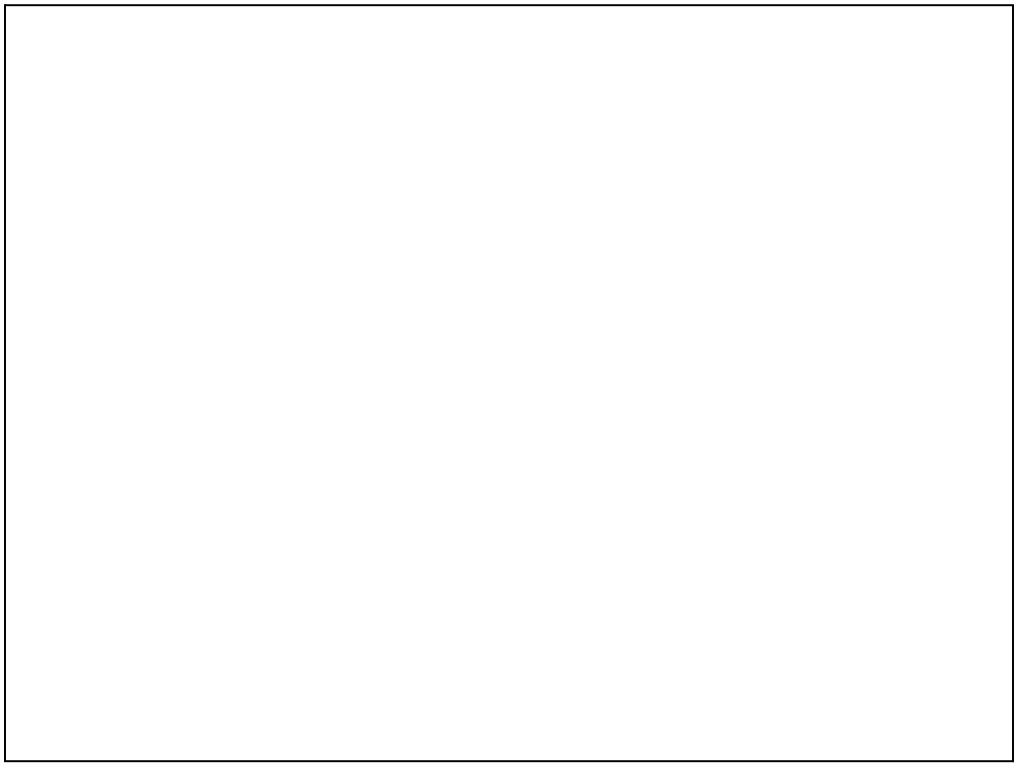


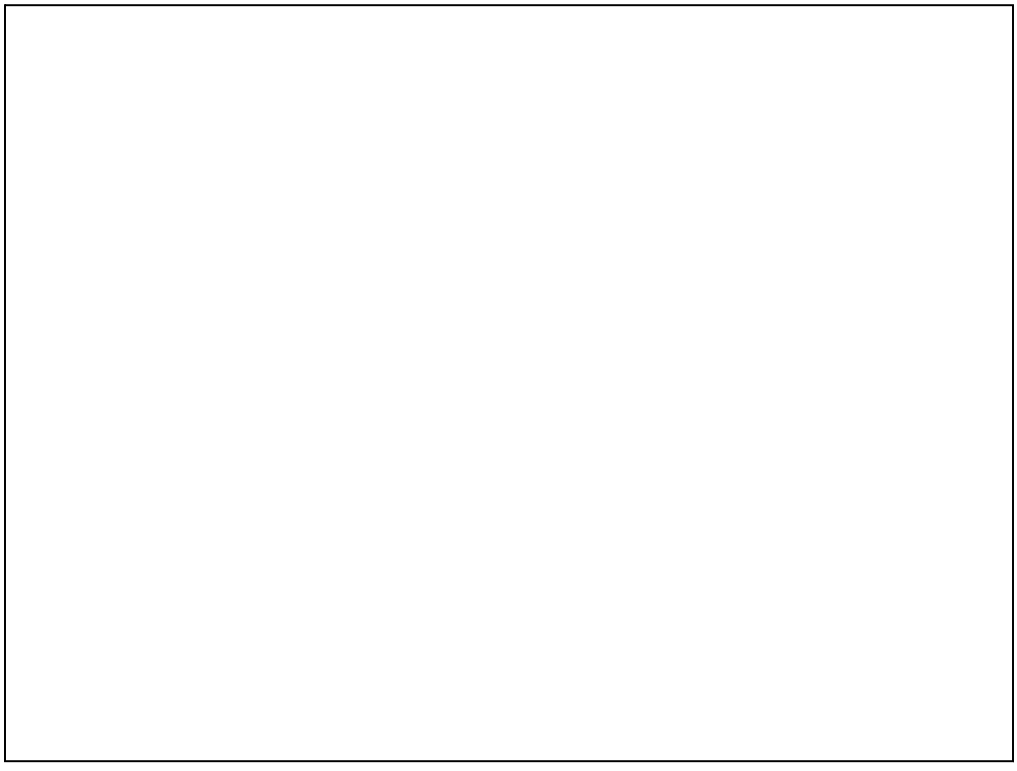


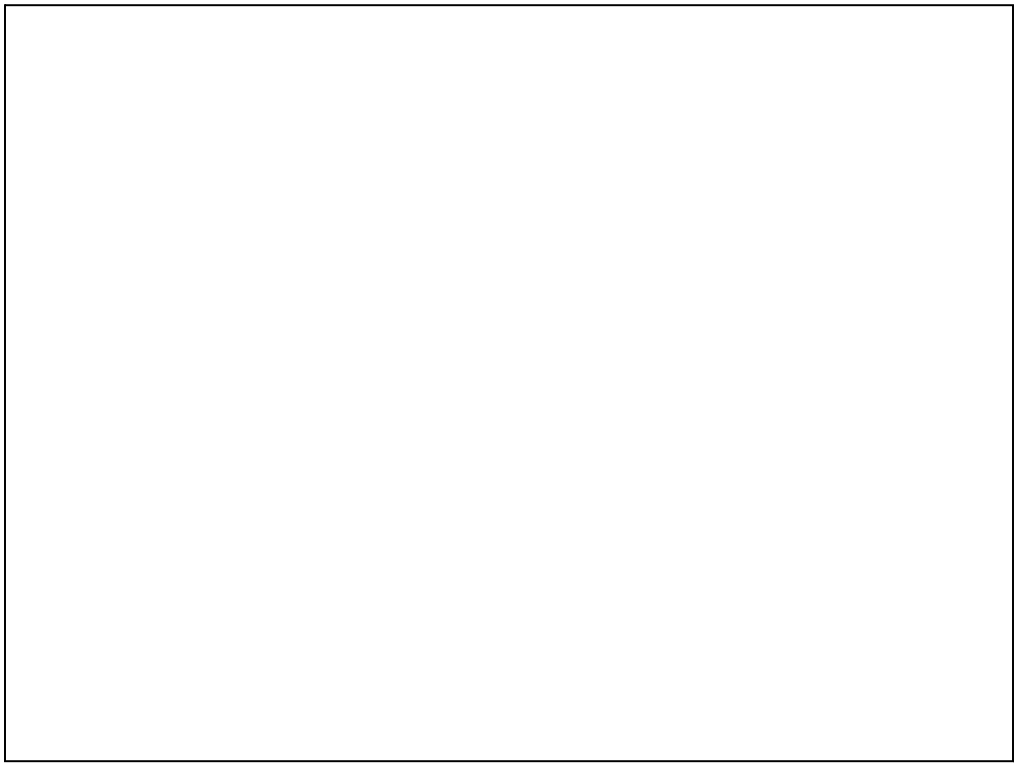


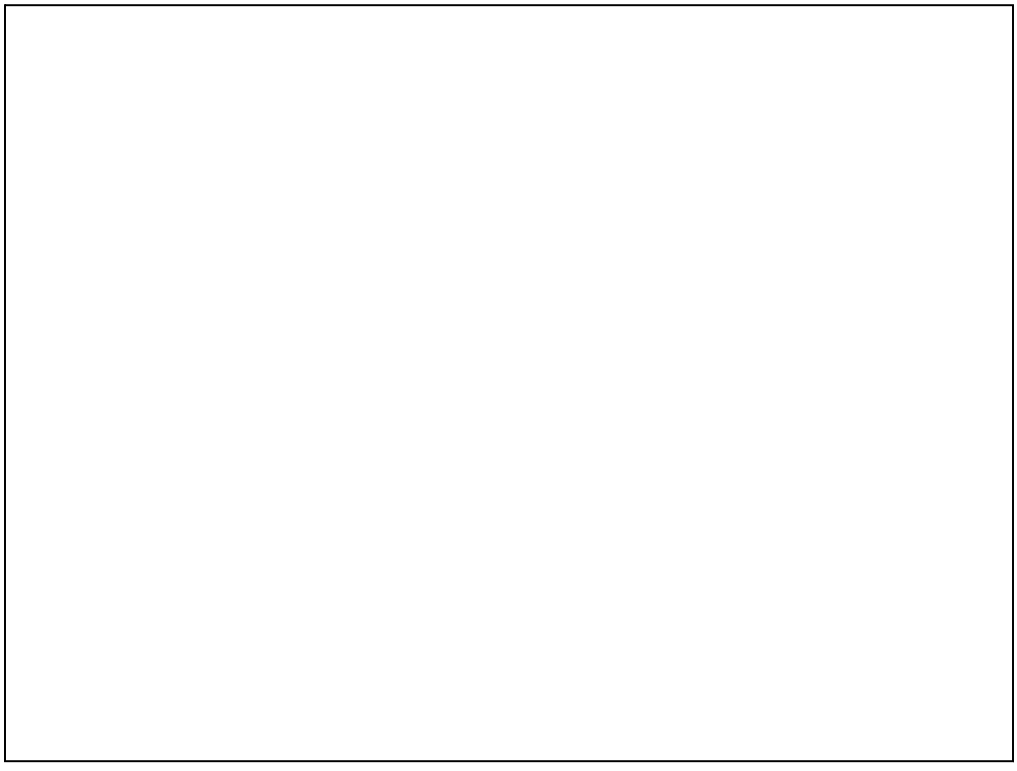
Ipv6 Anycast

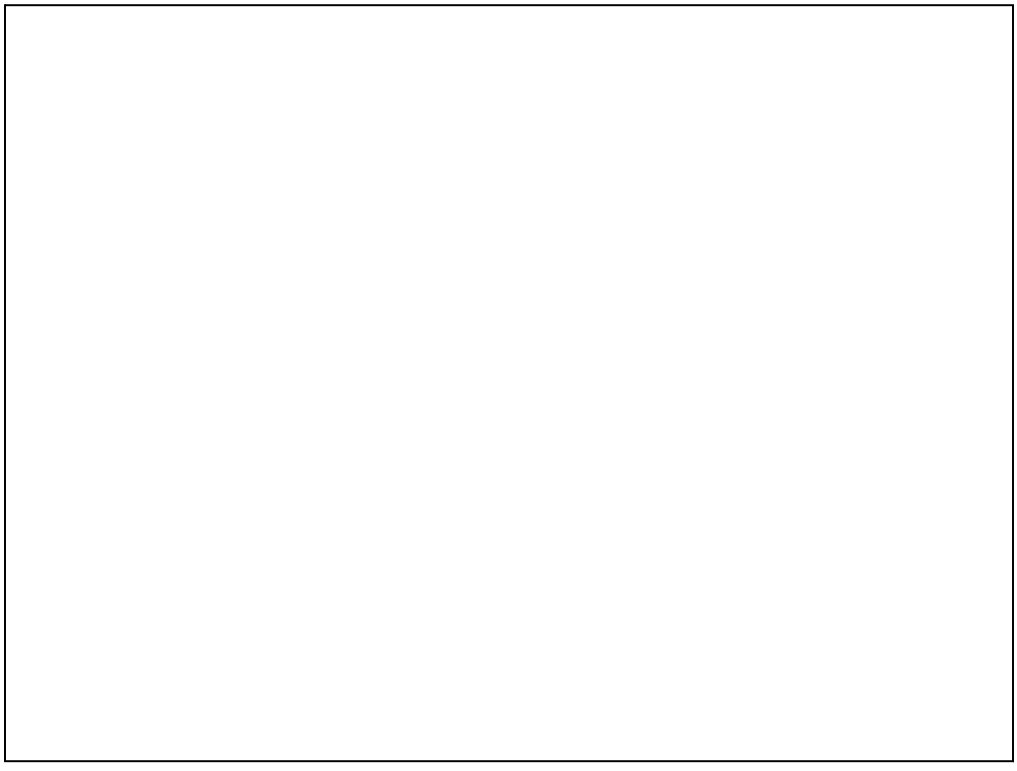
- Benefits
  - Anycast packet routed to "nearest" interface having that address, depending on distance along routing path
  - Service Abstraction
    - Anycast addresses can be used as service identifiers. Many services such as Domain Name System (DNS) and HTTP proxy could be accessed with anycast addressing
  - Reliability
  - Anycast address mechanism can be used for improved reliability of services
    - Anycast address can be assigned to servers scattered over Internet, a servers fails, other servers can still provide service



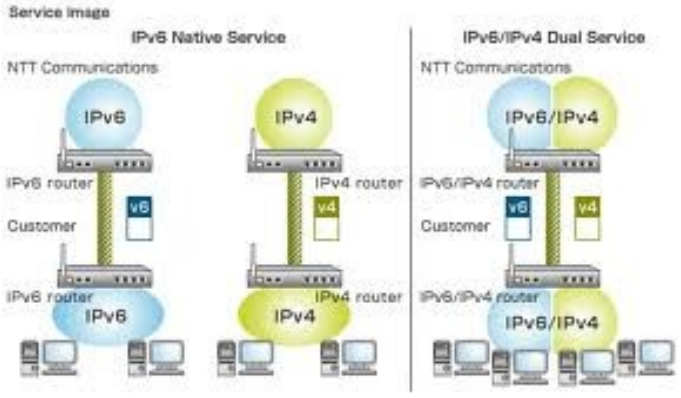


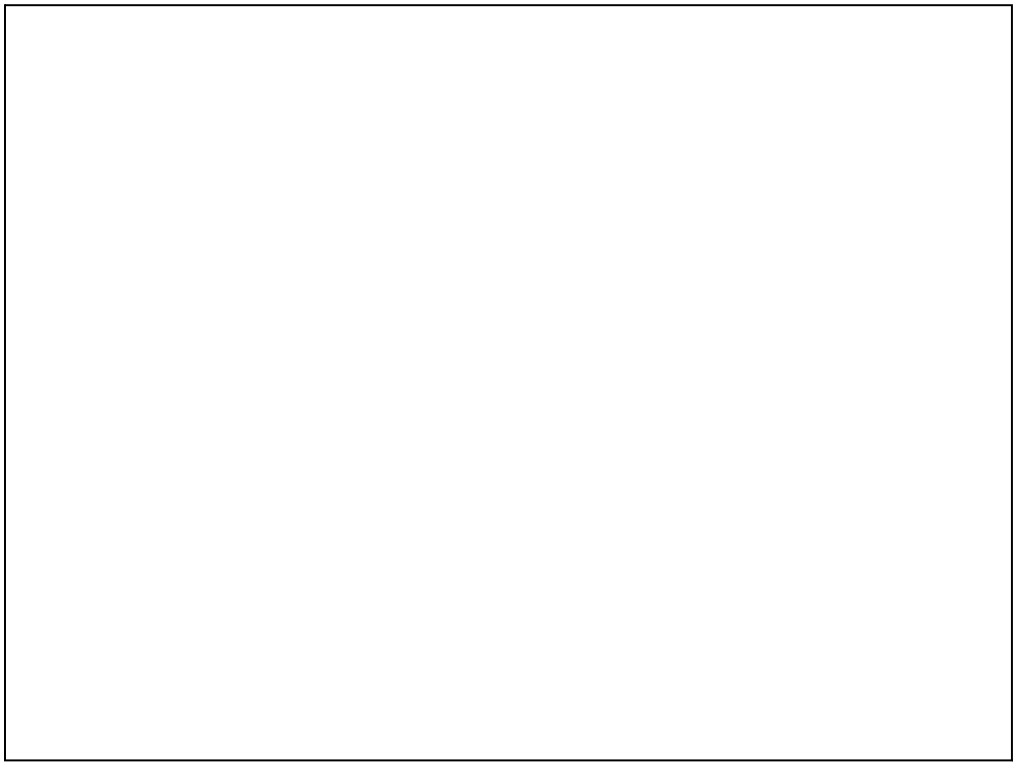


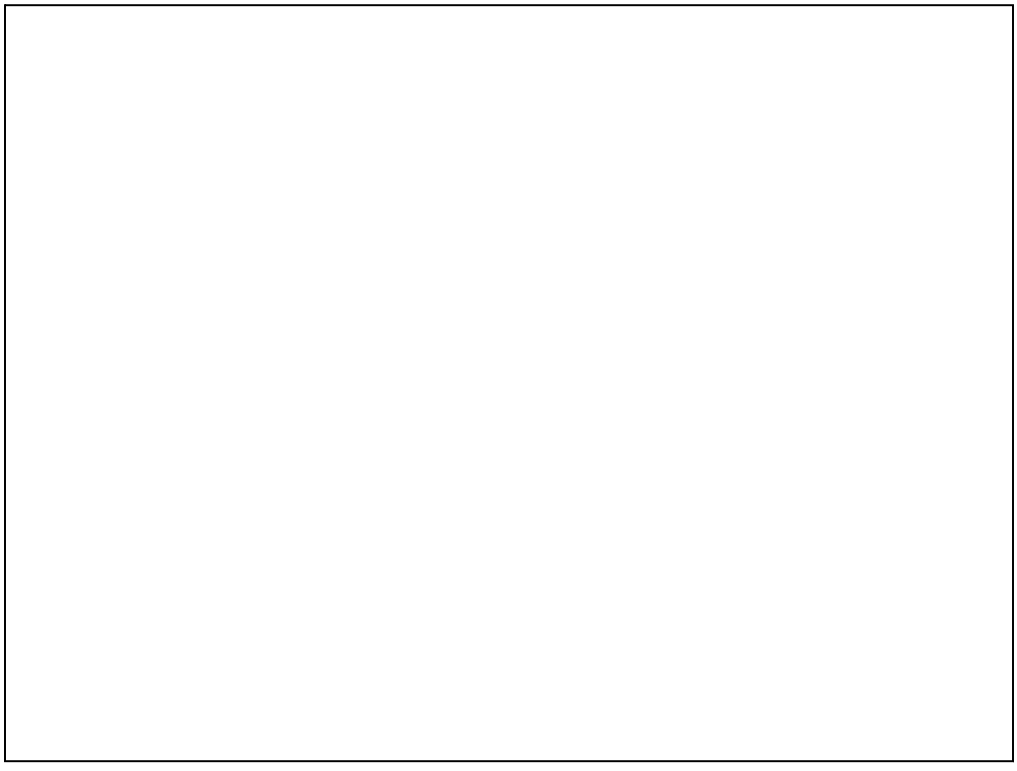


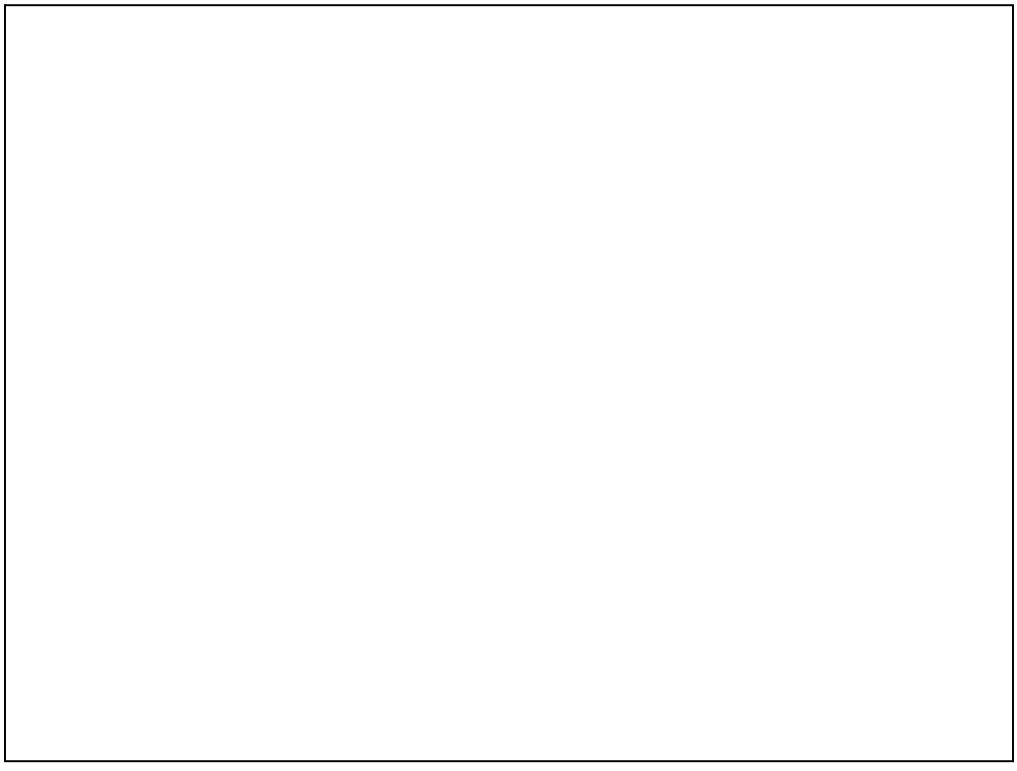


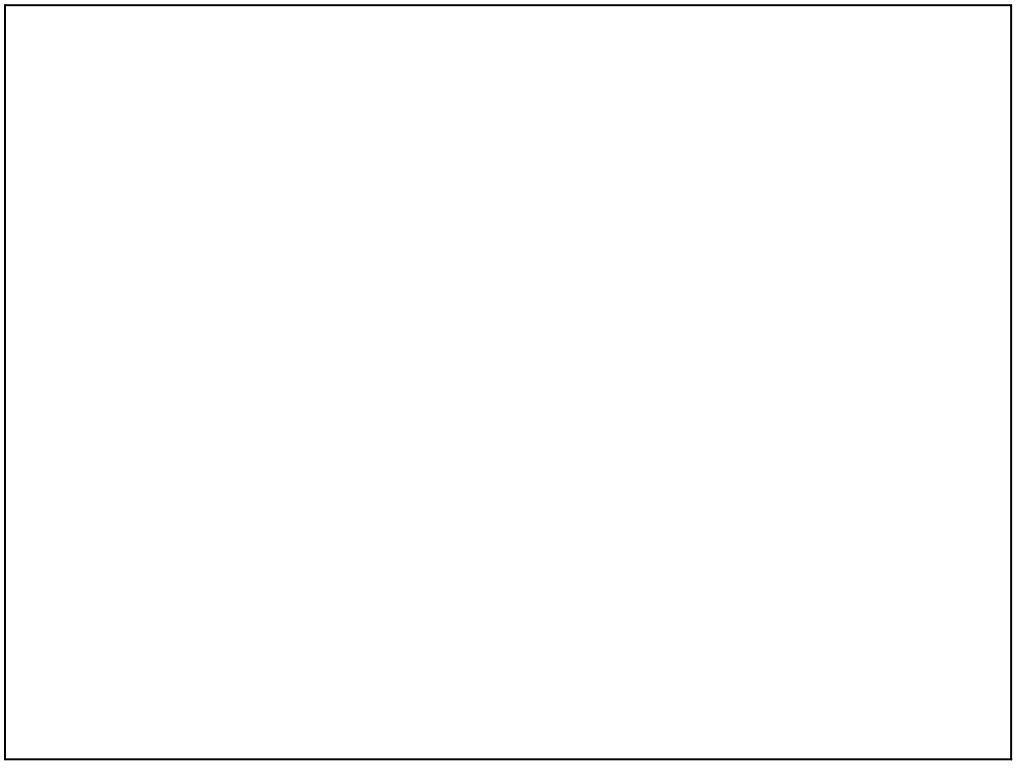
Dual Ipv6 and Ipv4 Service

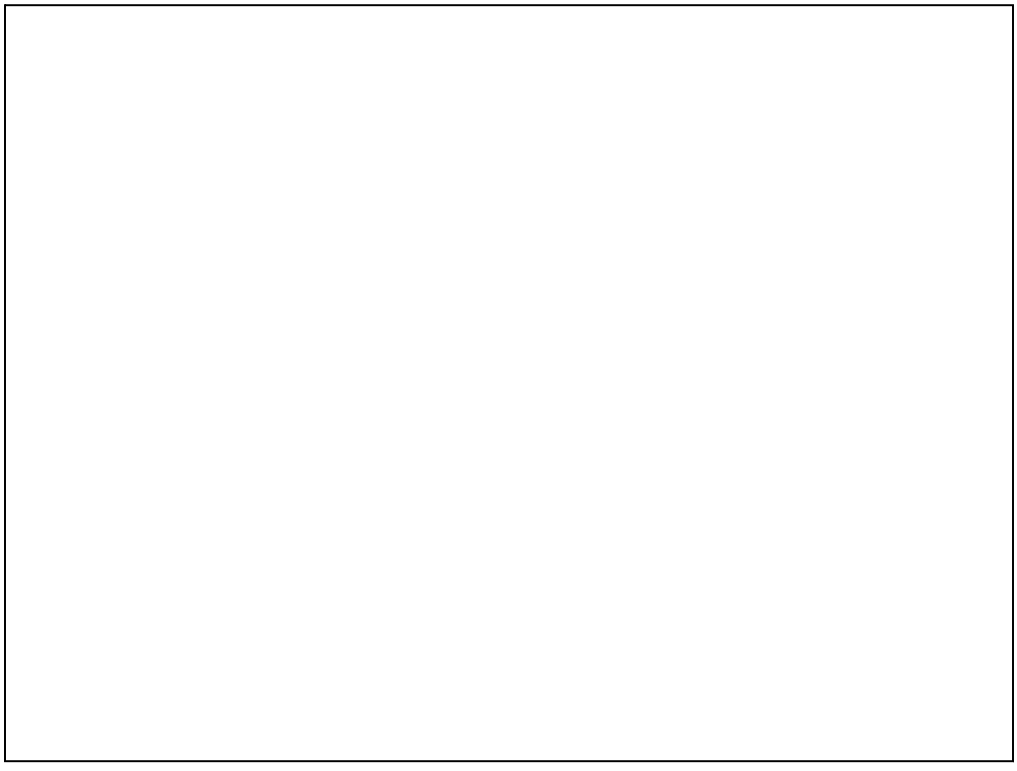


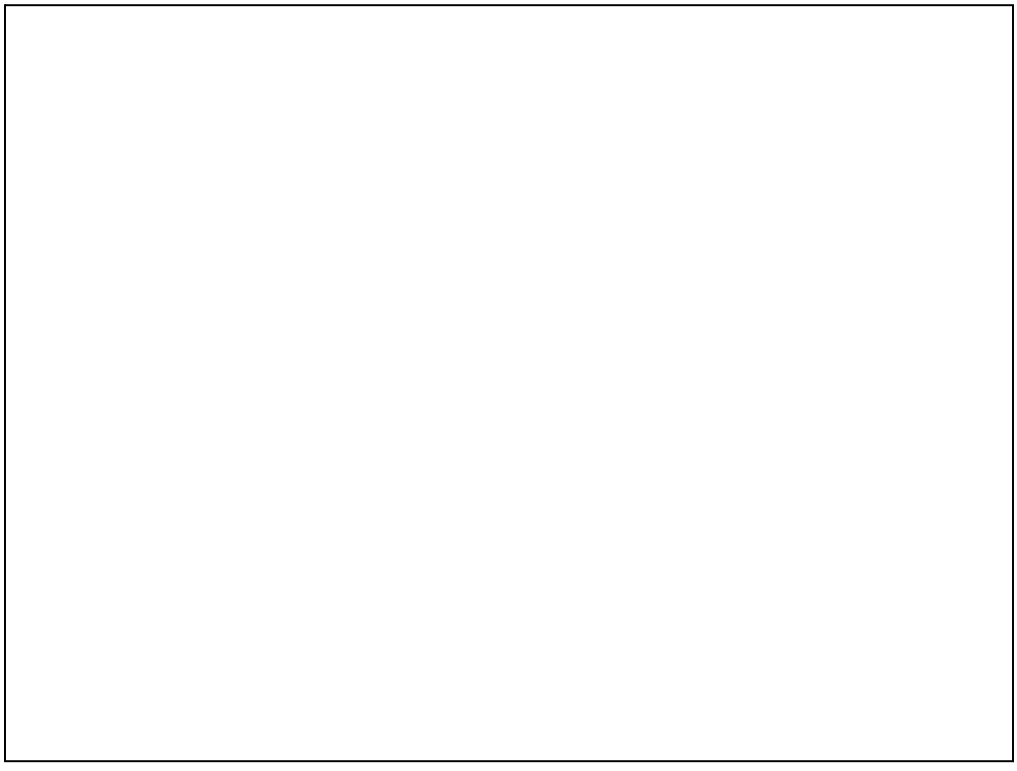


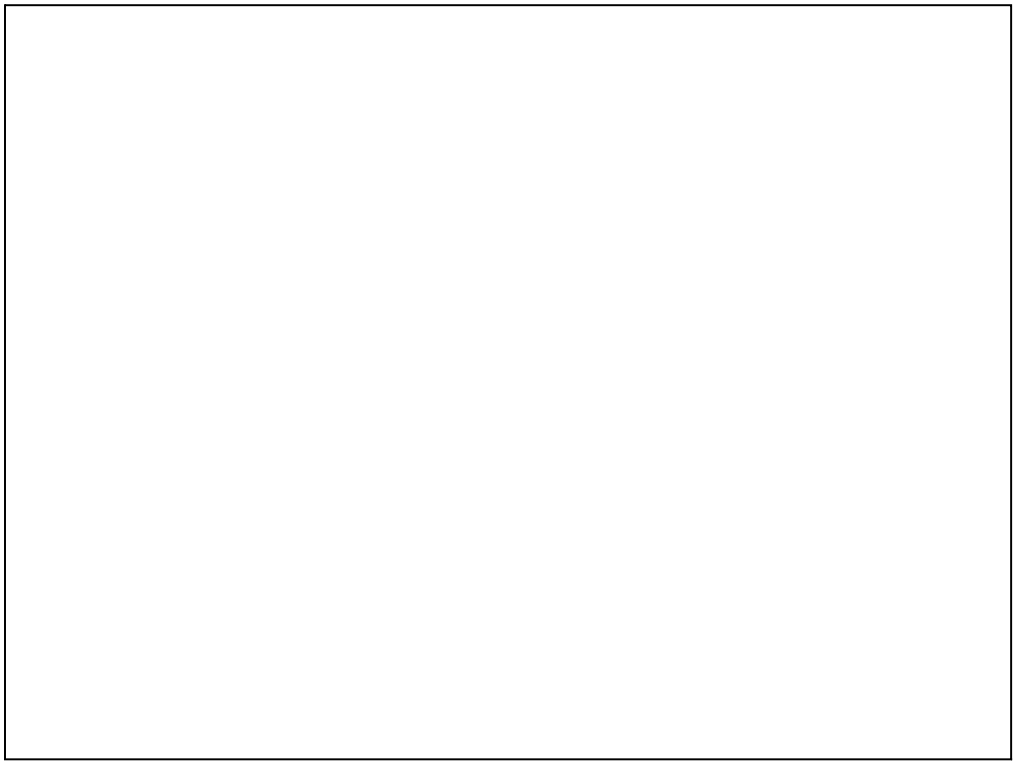


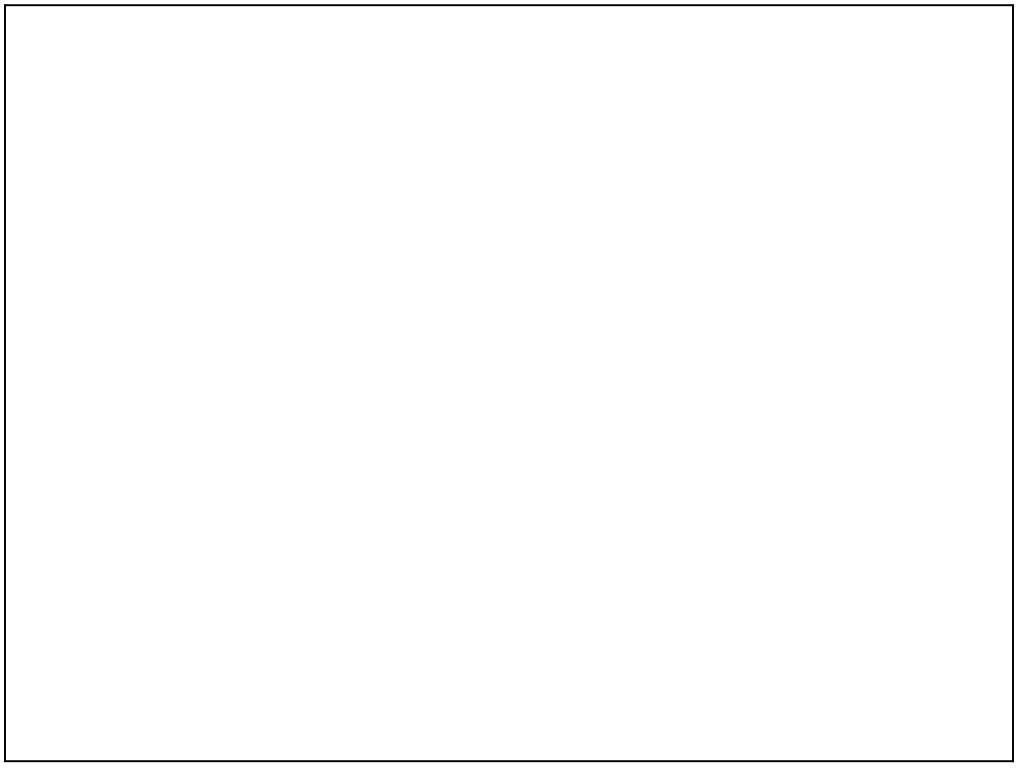


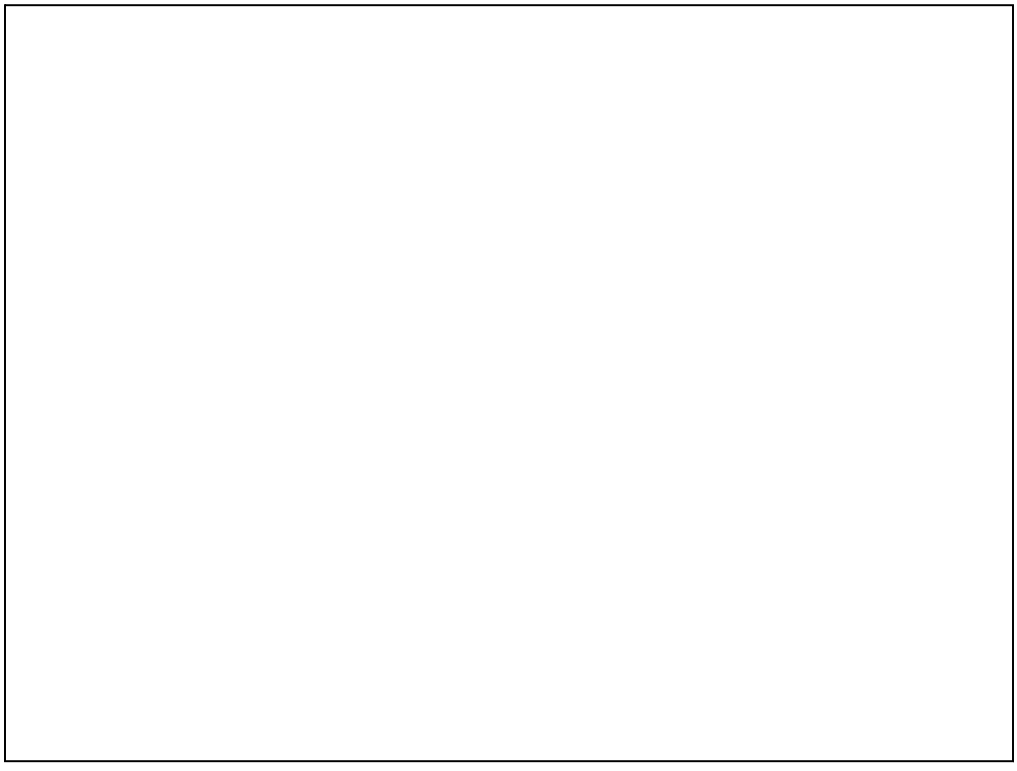


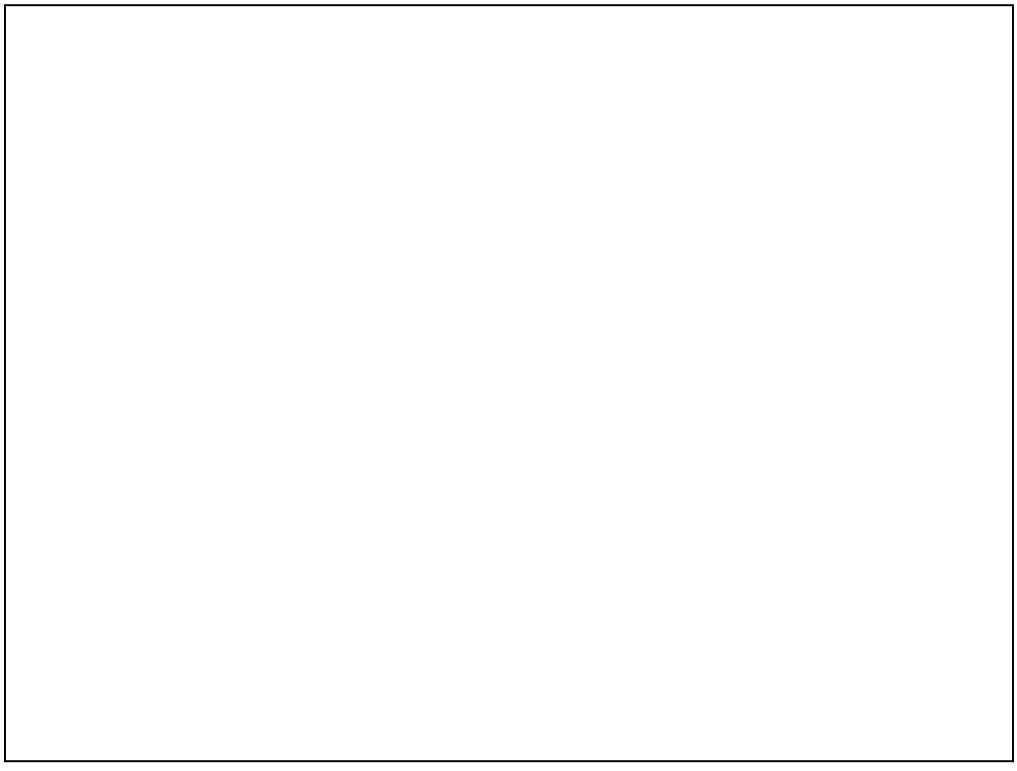












Security Issues in IP

- Source spoofing
- Replay packets
- No data integrity or confidentiality

Threats

- Attacks
- DOS attacks
- Replay attacks
- Spying
- and more…

Fundamental Issue:

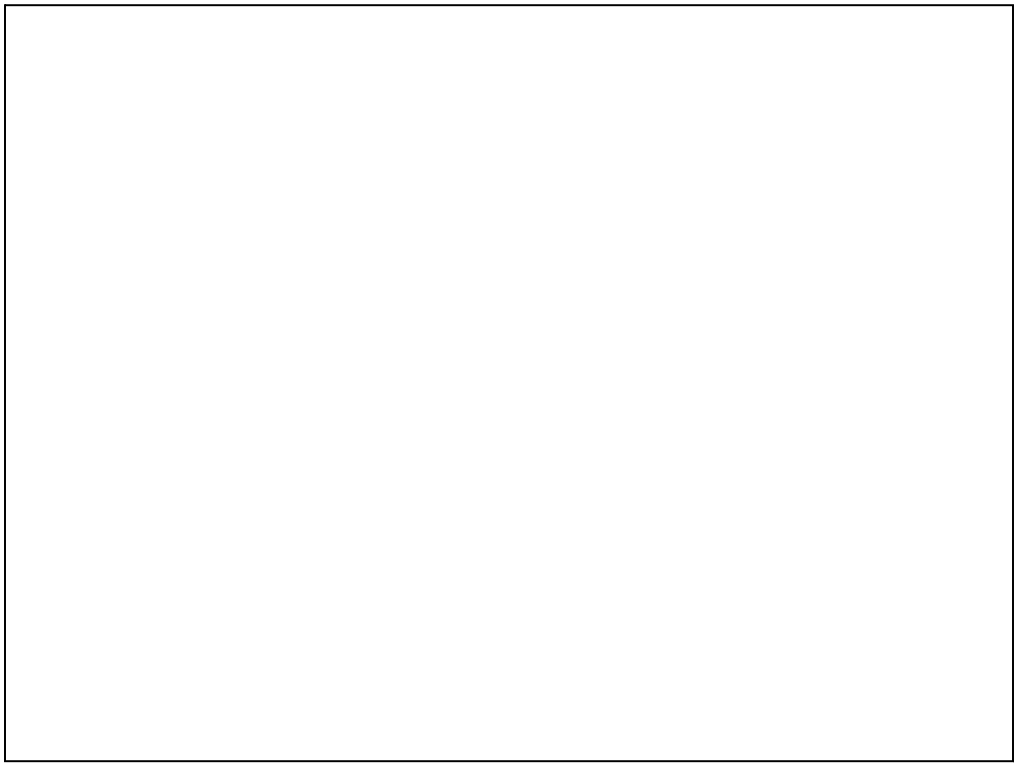
Networks are not (and will never be) fully secure

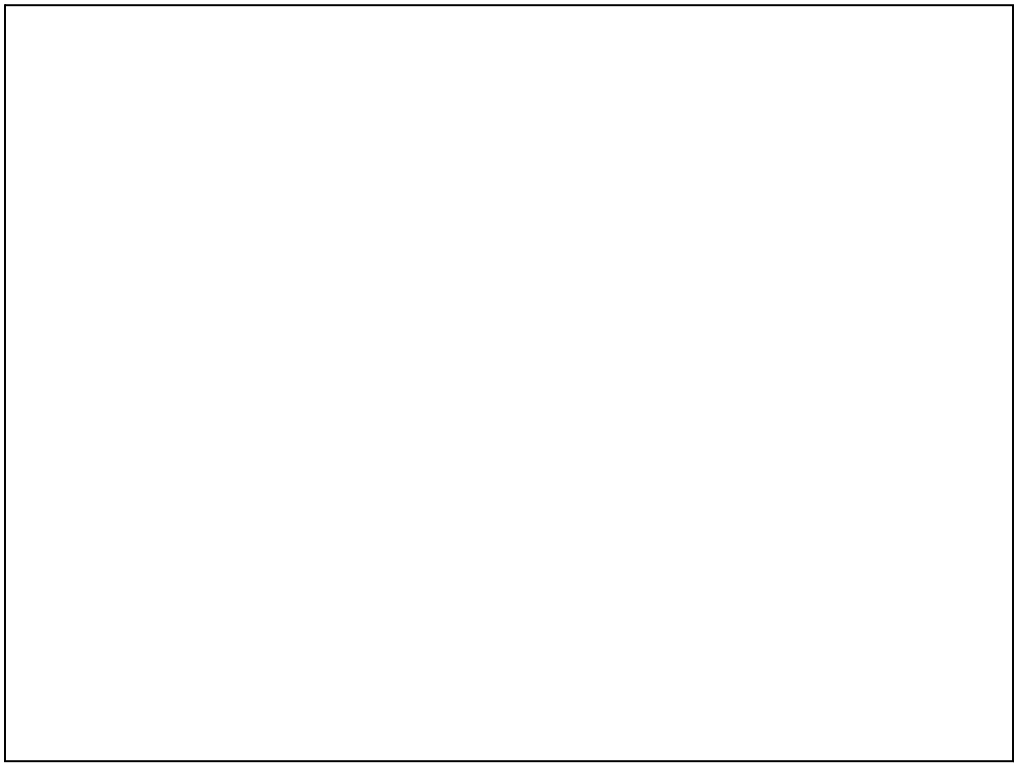
Goals of IPSec

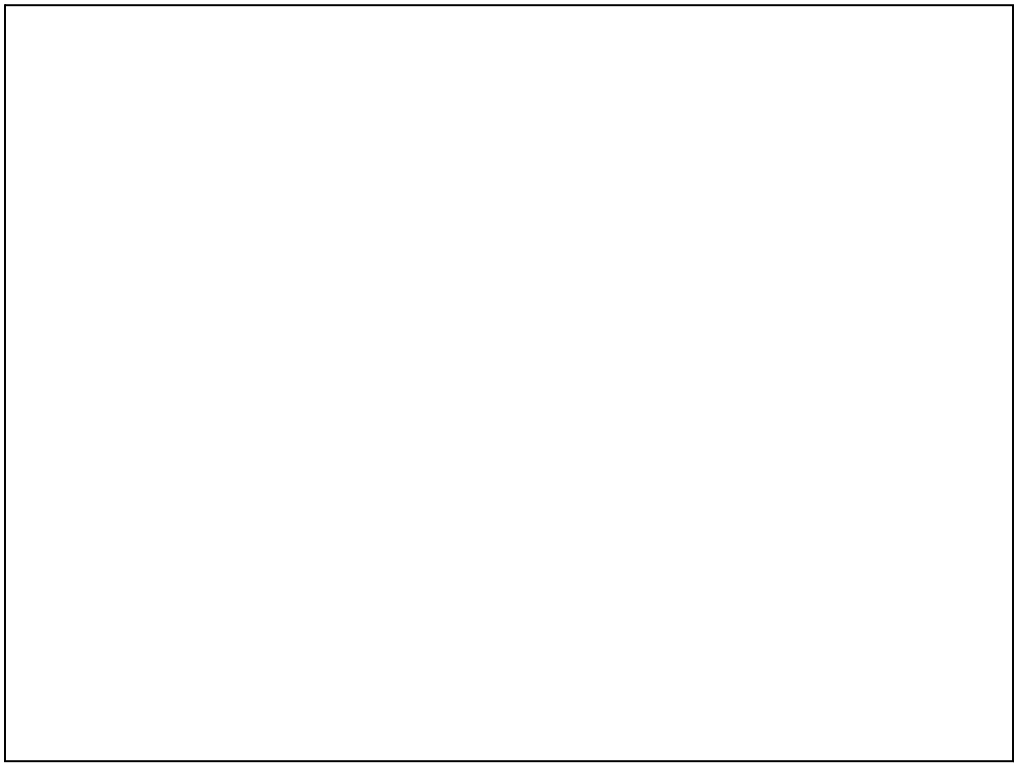
1. Verify sources of IP packets
   Authentication
2. Protect integrity and/or confidentiality of packets
   Data Integrity/Data Encryption

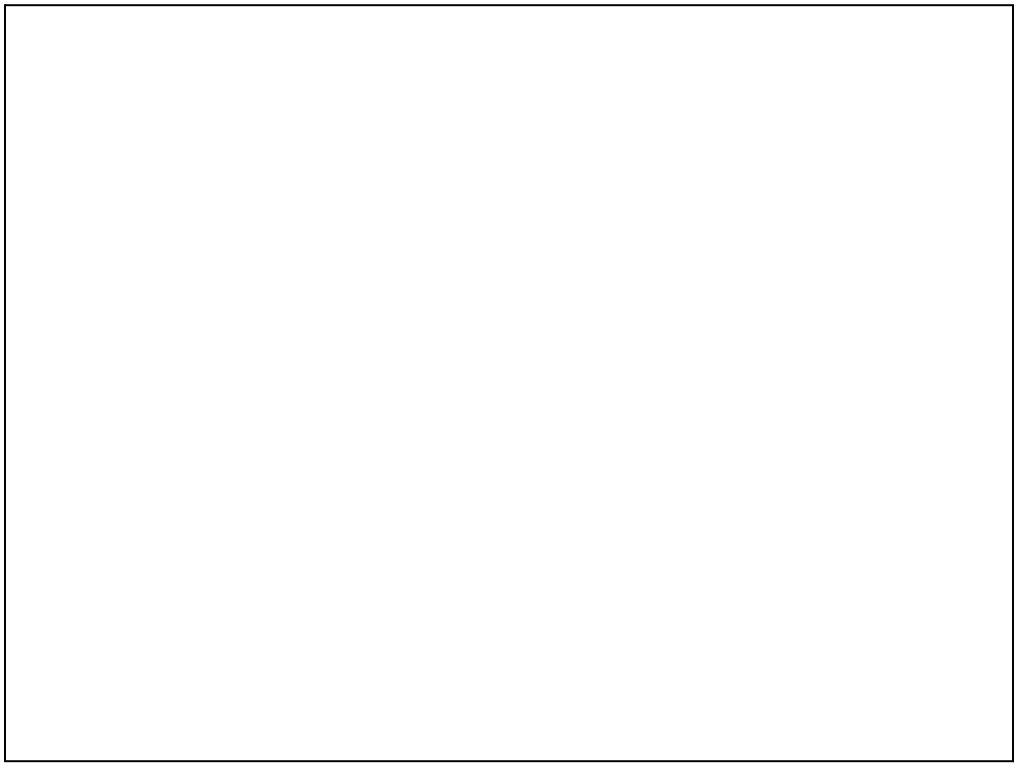
References

Illustrated Guide to IpSec
http://www.unixwiz.net/techtips/iguide-ipsec.html
Wikipedia
http://en.wikipedia.org/wiki/IPsec









Questions for IPv6

Said … Ipv6 as a lot like Ipv4 not too many changes … but

- What other protocols need to change to accommodate Ipv6?
  - Think about all the associated protocols that work with Ipv4 that facilitate addressing and routing
  - There will need to be changes to these protocols
  - ICMP6, DNS6, DHCP6, BGP