" 

We as F5 Networks are a bit dissapointed, that IPv5 never Became The New Standard........

# NOW
# IT'S TIME FOR IPV6

Jürg Wiesmann

Senior System Engineer F5 Networks Switzerland

j.wiesmann@f5.com

NOW IT'S TIME FOR IPv6!

ACTUALLY IT IS TIME FOR LUNCH RIGHT NOW, SO I FEEL VERY HONORED, THAT YOU ARE TAKE YOUR TIME TO SNEAK INTO MY PRESENTATION TODAY ABOUT OUR VIEW OF IPv6.

YOU ALLREADY MADE AN IMPORTANT STEP INTO THE NEW FUTURE OF IPv6. THE NEXT GENERATION OF PROTOCOL. MY PERSONAL VIEW ON IPv6 REALLY IS IT SHOULD HAVE BEEN CALLED SOMETHING ELSE THAN IP,

SO SOMETHING MORE LIKE CP (COMMUNICATION PROTOCOL) SINCE NOT MUCH IS THE SAME AS IT WAS IN IPv4.

IN THE PAST YEARS I DISCUSSED IPv6 AT VARIOUS OCCASIONS WITH IMPORTANT ENTERPRISE AND SERVICE PROVIDER CUSTOMERS ARROUND EUROPE IN LOWER AND MIDMANAGEMENT LAYERS, AND I FOUND IT REARLY HAPPENING, THAT THESE LAYERS DID DECIDE TO DO THE STEP TO IPv6. I AGREE THERE ARE LOTS OF FRIENDS AND POSITIVE INFLUENCERS IN THE LOWER LEVEL OF THE ORGANISATIONS, BUT THE INITIAL DRIVE I SEE MOSTLY COMMING EITHER FROM THE BUSINESS OR FROM CIOS.

IPv6 PUTS A LOTS OF NEW REQUIREMENTS TO ORGANISATIONS IN TERMS OF SECURITY BUT AT THE OTHER END ALLOWS NEW WAYS TO COMMUNICATE AND INTERACT TOGETHER.

COMPANIES SEEING NAT AS A SECURITY FEATURE WILL LEARN IT THE HARD WAY, THAT NAT WILL REDUCE THERE AGILITY IN AND FOR THE FUTURE.

SERVICES LIKE SKYPE/WHATSAPP ASO. ARE REQUIRING CONNECTIVITY POINTS SOMEWHERE IN THE INTERNET, JUST TO INTERCONNECT USERS HIDING BEHIND NATED NETWORK BORDERS.
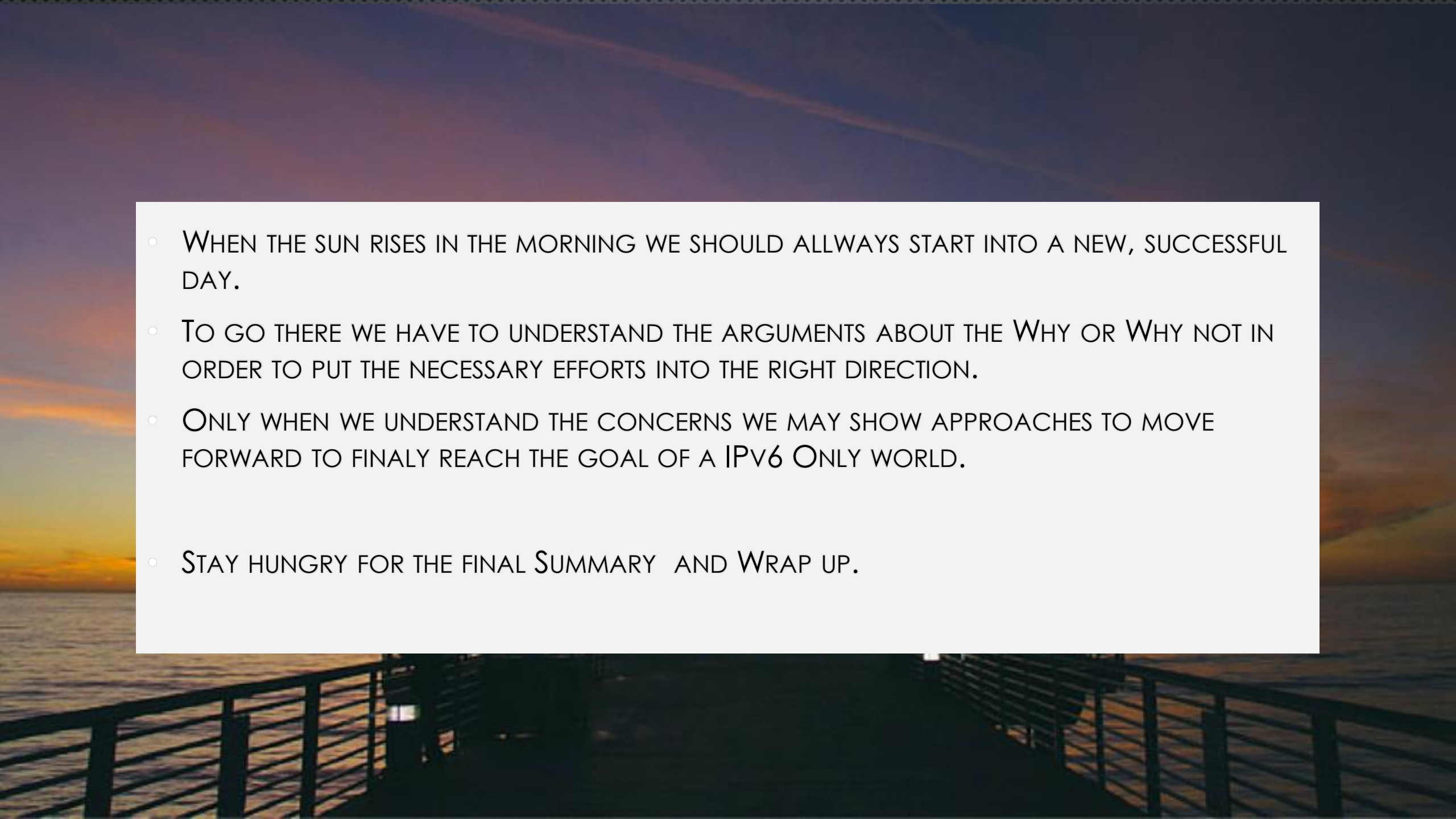
DEPENDENCYS WHICH SHOULD GO AWAY THE EARLIER THE BETTER.

IN THE UPCOMMING 45 MINUTES I WOULD LIKE TO TOUCH BASE WITH YOU AND SHARE WHAT I BELIVE ARE THE RIGHT APPROACHES TO DO IT.

# AGENDA

- **IPv6 State of the Union**

- **Approaches**

- **Goal**

- **Summary**

- When the sun rises in the morning we should allways start into a new, successful day.

- To go there we have to understand the arguments about the Why or Why not in order to put the necessary efforts into the right direction.

- Only when we understand the concerns we may show approaches to move forward to finaly reach the goal of a IPv6 Only world.


- Stay hungry for the final Summary and Wrap up.

WHY (NOT) NOW...

# WHY (NOT) NOW...

Going through IPv6 with my Customers always bring lots of arguments to the Table on why an IPv6 Migration is not possible and not required. In Addition even we understand about the OSI Model, mostly we are afraid of a migration, since no certainty exists, that Applications do not contain any Network Or Session dependencies.

Since it is definitively true, that most of the Applications are internal where there are enough IPs. The view on the DMZ or Public Facing Applications should be a different one.

Very recently I was talking to a Customer who moved into new Datacenters, about the why they did not move or build an IPv6 ready Datacenter. They did just talk to the Application owners....

..... and they did not have a Requirement for IPv6 jet, and since IPv4 works and is proven for years, IPv6 is rather complicated why should he go for a change ?

Another Concern I often hear is, it is impossible to remember IPv6 Addresses, and the dependency on DNS is huge.

The biggest concern and this sounds really understandable is that most of the Companies are concerned and they are not really sure if there Applications would still work with IPv6.

.......Never Touch a Running System

Last but not least Security is a «challenge», Products and technology proven in IPv4 might not be as reliable and secure, when building them using IPv6. In addition protocols like ICMP which where normally blocked in IPv4 Environments are suddenly required when using IPv6.

And the Difference of the Protocol i.e. Protocol Extension Headers are clearly seen as a risk.

And if Infrastructure Components are not built for IPv6 Performance could decrease dramatically.

Certainly in IPv6 mostly Auto configuration may be used, so Administrators and Security responsible are afraid of loosing the context of the user to Application.

Others state, that they want to have the coexistence of IPv4 and IPv6 as short as possible. They want to go there, but just not NOW.


It is a long way to full IPv6 the concept comes first, a clear strategy and a concept and a clear goal needs to be specified before the Steps can be taken.


IT has a Lifecycle so what about using the lifecycle to migrate to IPv6.

If new applications are deployed, they should get deployed using PURE IPv6. So plan, if you did not already, and build your IPv6 World in your Datacenter.

If you role out new Clients or new Operating Systems do it in IPv6.

Why not...... Why not start today.

WHY NOW

# WHY NOW

IPv6 is reality, and you may not blow the fact into the Wind, that you will have to do it! better sooner than later.

I understand that running two protocols in the networks might not be desired, but this is something we ALL will not be able to work arround it.

Looking at IoT it is reasonably clear, that this Technology deployments will be based on IPv6. This Devices need to be controled over the internet or through a (LPN) Low Power Network , so NAT is not feasible and only IPv6 will be capable to scope with this large number of Devices.

In addition there is a huge drive to allow the other 5 Billion of the wold Population access to the internet. (Project Loom from Google) Today only 46% of the World Population has access to the internet. (Internetlivestats.com)

They all will have there Direct Access to the internet, will require there own IP aso.

As of today Service Providers are allready fully IPv6 aware and are using CGNAT Devices to translate legacy IPv4 Traffic to IPv6 and back. This introduces latency and as soon as over 50% of the Traffic on the internet are IPv6

The use of IPv4 is a clear disadvantage.

I agree to a certain degree, the risk of moving current Platforms and Applications to IPv6 is a path, nobody would wants to take.

Doing this during a Software/Platform Lifecycle how ever is a riskfree and non distruptive approach and will make the move to IPv6 Seamless without any issues.

You are right Clients and DNS Infrastructure will be Dual Stack for Years, and it is key to manage IPv6 migrations and management seamless to the subscribers, where translation between IPv4 and IPv6 Networks are not causing a bottle neck.

To successfully manage these translations along with managing other IP services, such as: DNS, NAT, Security Policy the right tools and expertise is necessary, and if Clients are Infrastructure (Firewalls / Proxys / Switches / Routers / Apps aso) needs to stay IPv4 capable.

If you decide to stay IPv4 till you are forced to move, you are going into a uncontrolled and uncertain future.
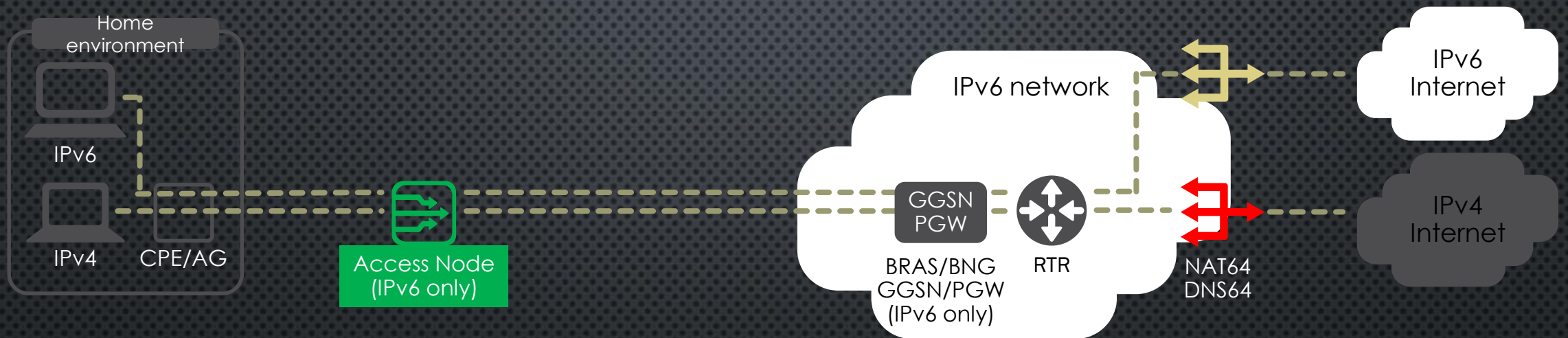
Today IPv6 looks like the Island.... (But this Island grows fast.....)

In the Future the Island should not be you

Let me give you some examples to proof this will happen

# NETWORK MIGRATION
## NAT64



Home environment

IPv6

IPv4          CPE/AG

Access Node (IPv6 only)

IPv6 network

GGSN PGW

BRAS/BNG GGSN/PGW (IPv6 only)

RTR

NAT64 DNS64

IPv6 Internet

IPv4 Internet

Cost-effective and scalable
Lower CapEx / OpEx

Geographic High Availability
High Speed Logging

# NETWORK MIGRATION
## NAT64

- Here you may see an actual real world example of todays Service Provider Networks.
- As of today, they are allready IPv6 to the Access Node providing IPv6 to the Access Node

- The On Premise Environement either IPv4 or/and IPv6 will run through the CPE and will be translated to IPv6

- Due to the Fact, that Destination addresses will be on the IPv4 World another Translation would have to take place before going to the «IPv4 Internet»

- A IPv6 System will not need to be translated in the Access Node or CPE and will be transfered to the IPv6 Network to either directly to the IPv6 Internet or translated to IPv4.

- You may turn it back and forth going for IPv6 will reduce the number of translations.

# Supporting IPv6 in iOS 9

August 28, 2015

At WWDC 2015 we announced that iOS 9 will support IPv6-only network services. All apps submitted to the App Store must support IPv6 starting in early 2016. To make sure your app is compatible, use the networking frameworks (e.g., "NSURLSession"), avoid use of IPv4-specific APIs, and avoid hard-coded IP addresses. Before submitting your app, test for compatibility.

To learn more, read Supporting IPv6 DNS64/NAT64 Networks and watch Your App and Next Generation Networks.

**APPLE APPSTORE**

1'745'873'632'255

1'675'068'324

# INTEROPERABILITY

# INTEROPERABILITY

- INTEROBERABILITY IS THE FEAR WE ARE SHARING BUT SEVERAL TECHNICS EXIST TO MAKE INTEROPERABILITY WORKING.

- ON CLIENTSIDE MOSTLY USED ARE DUAL-STACK TECHNIQUES. THEY ALLOW IPv4 AND IPv6 TO COEXIST ON THE SAME DEVICES AND NETWORKS

- SOMETIMES (RARELY) LIKE TEREDO AND ISATAP TUNNELING TECHNIQUES ALLOW AND HELP TO TRANSPORT IPv6 TRAFFIC OVER AN EXISTING IPv4 INFRASTRUCTURE.

- UNFORTUNATELY THIS IS NOT POSITIVELY TAKEN BY SECURITY, SINCE IT MAKES IT HARD TO CHECK, WHAT IS TRANSPORTED WITHIN THE TUNNEL, AND EVEN WORSE WHAT IS DONE AT THE END OF THE TUNNEL.

- IN ADDITION THIS CAUSES ADDITIONAL OVERHEAD AND WILL AFTER ALL NOT PROVIDE THE COMPLETE FEATURESET REQUIRED BY THE IPv6 CLIENTS.

- LAST BUT NOT LEAST TRANSLATION TECHNIQUES (GATEWAYS) ALLOW IPv6-ONLY NODES TO COMMUNICATE WITH IPv4-ONLY NODES AND VICE VERSA. THE BENEFIT OF THIS TECHNOLOGY IS THAT NEITHER INFRASTRUCTURE MUST BE TUNED AND MODIFIED AND THEY MAY COEXIST MOSTLY INDEPENDANT DURING THE MIGRATION PHASE.

- HOW EVER, EVEN LOTS OF INTEROPERABILITY MECHANISM EXIST TODAY, THE INITAL STEP TO DO IPv6 SEAMS TO BE TO BIG FOR A LOT OF ENTERPRISES.


- THIS BRINGS ME TO A NEW IDEA.

- WHO IN HERE HAS A CLOUD PROJECT OR INITIATIVE RUNNING ?

# IPV6 CLOUD

# IPV6 CLOUD

- Many Companies these Days are going for Cloud now, or have at least a clear strategy or initiative to go to the cloud..

- Either IaaS/PaaS or SaaS Solutions are provided more and more to reduce Costs by sharing ressources.

- Maybee moving Applications to the cloud is a good starting point to implement IPv6.

- To make an Application Cloud Ready several steps and detailed Tests are necessary to bring a Application to the Cloud.

- If we would build the Cloud Infrastructure based on IPv6 and migrate the Application to this cloud, 2 Steps may be taken at a time.

1. You can assure your newly deployed Application is IPv6 Ready

2. Your existing Application Infrastructure is not touched.

Unfortunately IPv6 is not commonly offered in Clouds like AWS or Azure, but other Cloud Offerings or your Private Clouds are more flexible ?

So if you are sitting in this room and are having a cloud offering for your customers, think about this Unique Selling Point and if you are currently planning to go

for a Cloud Based Solution put IPv6 as a Key Requirement on the list before signing up to a cloud solution.

But how will you migrate your Users/Apps within your Infrastructure ?

START BUILDING ISLANDS

IPv6 User

Todays IPv4 Infrastructure

Int. IPv6 Apps

DMZ

# START BUILDING ISLANDS

- Thinking about Migration is like thinking or building Islands.

- Today there is a big Island in the middle having all of your Users and Applications most potentially using IPv4 on the Application Side, but beeing Hibrid on the Client Side.

- Mostly the DMZ with all the Internet Facing Application is migrated to IPv6 require to resolve DNS Requests for a AAAA Record with an IPv6 Address and DNS Requests for a A Record using the original IPv4 Address,

- If you have a Client Renewal Project running, you might want to build these new Systems using a IPv6 Stack only using features like Autoconfiguration aso.

- If you are having a Application Lifecycle Process the move to Pure IPv6 is key. This will ensure, that the Application is fully IPv6 aware and has no IPv4 Interaction with other Systems you are not aware of.

- These Applications should be carefully tested using IPv6 only Workstations with individal Operating Systems/Browsers before they are proofen to be IPv6 Capable.

- After these Islands are built the Necessary Bridges have to be built to allow the interconnectivity between the IPv4 and IPv6 World

# THE BRIDGE

- **DNS (DNS64)**
- **IPv4 / IPv6 Gateway**

# THE BRIDGE

Building the Bridge between IPv6 and IPv4 requires 2 important Pillars.
DNS and Protocol Translation/Gateway Functionality.
DNS64 and DNS46 but also NAT46 and NAT64.
Let me explain in the following Slides how this Bridge would help your IPv6 Client to connect to the Application

- **DNS (DNS64)**
- **IPv4 / IPv6 GATEWAY**

# IPV6 AND IPV4 SUPPORT INCLUDED

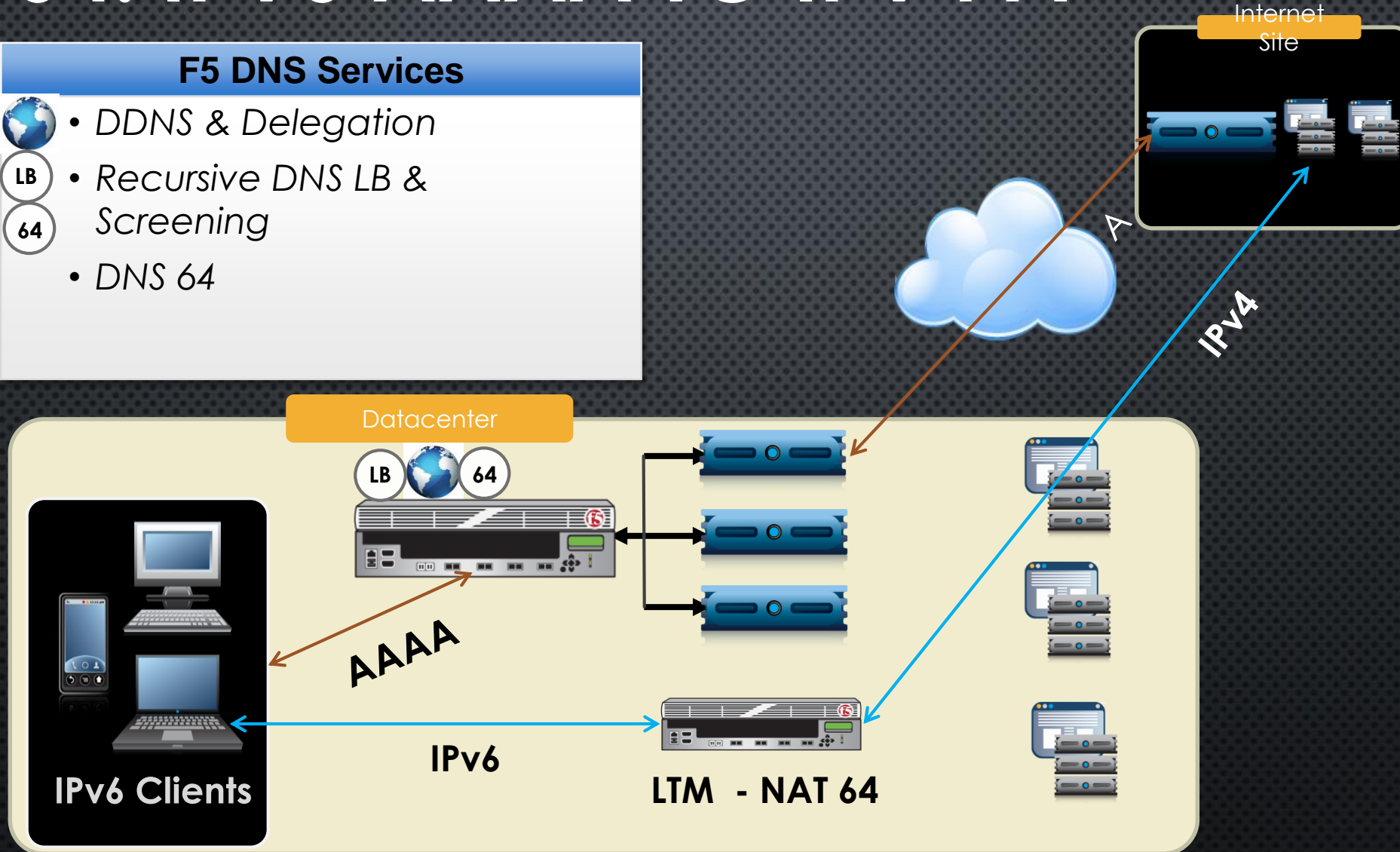## SIMPLIFY IPV6 MIGRATIONS WITH AN IPV4 / IPV6 GATEWAY

IPv4 → IPv6

IPv6 → IPv4

www.foo.com

- No need to tunnel

- "no dual stack clients or servers required"

- NAT IPv4 to IPv6 (and vice-versa)

  - Clients can be a mix of IPv4 and IPv6

  - Servers can be a mix of IPv4 and IPv6

- DNS 4-6 / 6-4

# DNS 64: IPV6 AAAA TO IPV4 A

DNS 64 and NAT 64 together provide an alternative way to deploy pure IPv6 clients while still maintaining connectivity to the mostly IPv4 internet.

The clients request pure IPv6, AAAA records.

The DNS 64 function either resolves an actual AAAA response or it synthesizes a AAAA response containing an embedded IPv4 A record.
In the case of a synthesized AAAA response, the client connects to the NAT 64 BIG-IP which initiates an IPv4 connection to the internet site.
The BIG-IP communicates with the internet site using IPv4 and communicates with the IPv6 clients using only IPv6.

Path MTU discovery is optional in IPv4 but mandatory in IPv6. If an IPv4 host does Path MTU discovery by setting the Don't Fragment bit in the header,
Path MTU discovery works even through the translator.
The sender may receive Packet Too Big messages from both IPv4 and IPv6 routers.

If the Don't Fragment bit is not set in the IPv4 packet, an IPv6 translator has to ensure that the packet can safely travel through the IPv6 network.

It does this by fragmenting the IPv4 packet if necessary, using the minimum MTU for IPv6, 1280 bytes.
IPv6 guarantees that 1280-byte packets will be delivered without a need for further fragmentation.

In this case, the translator always includes a fragment header to indicate that the sender allows fragmentation.
Should this packet travel through an IPv6-to-IPv4 translator, the translator knows it can fragment the packet.

For a UDP packet with a zero checksum, the translator must calculate a valid checksum for IPv6. If a translator receives the first fragment of a fragmented UDP packet with a zero checksum,
it should drop the packet and generate a system message specifying the IP address and port number. Further fragments should be silently discarded.

SHORT MIGRATION ?

SEAMLESS AND TESTED

# SHORT MIGRATION ?

IS THERE A WAY TO A SHORT MIGRATION ?

PROBABLY NOT....
IF YOU HAVE YOUR ADDRESSING CONCEPT READY, AND YOUR BASE INFRASTRUCTURE IS IPV6 READY, AND YOU HAVE A CLEAR AND STRICT STRATEGY TO DEPLOY NEW APPLICATIONS IN PURE IPV6.

- YOUR NEW APPLICATIONS MAY BE IPV6,
- SAVELY TESTED BEFORE USERS ARE CONNECTED TO IT
- AND BY TAKING THIS APPLICATION LIFE AND THE LEGACY APPLICATION OFFLINE YOU MADE A SUCCESSFUL STEP TO YOUR PURE IPV6 FUTURE.


- SO THE MIGRATION SHOULD BE SEAMLESS AND TESTED...
- TESTS SHOULD INCLUDE:

- IPV4 CLIENT SHOULD ACCESS THE APPLICATION (FULLY TEST THE APPLICATION, MAKE SURE NOTHING IS CACHED ON THE CLIENT I.E. DNS ADDRESSES / BROWSER CACHE / NETBIOS ASO...) ENSURE AUTHENTICATION / AUTHORISATION TO THE APPLICATION WORKS AS EXPECTED. IN ADDITION THE TRAFFIC SHOULD PASS ROUTERS AND FIREWALLS.
- IPV6 CLIENT SHOULD ACCESS THE APPLICATION. MAKE SURE SERVER AND CLIENT ARE NOT IN THE SAME IP NETWORK WHEN TESTING, AND A STATEFUL FIREWALL IS IN PLACE.

Allready a long yourney

There is a bumpy Road ahead of us.

The Migration will where ever it starts not be as Quick as you would wish.
Security Concepts are currently or need to be reworked based on the Zero Trust Model.
So Security needs to be more Context aware and Firewalls need to be configured using DNS based ACLs since IP Adresses are not as Static as you would see them.

Traffic Relations will no longer relay on NAT so Direct Communication between Endsystems (Users and Applications) should be controlled.
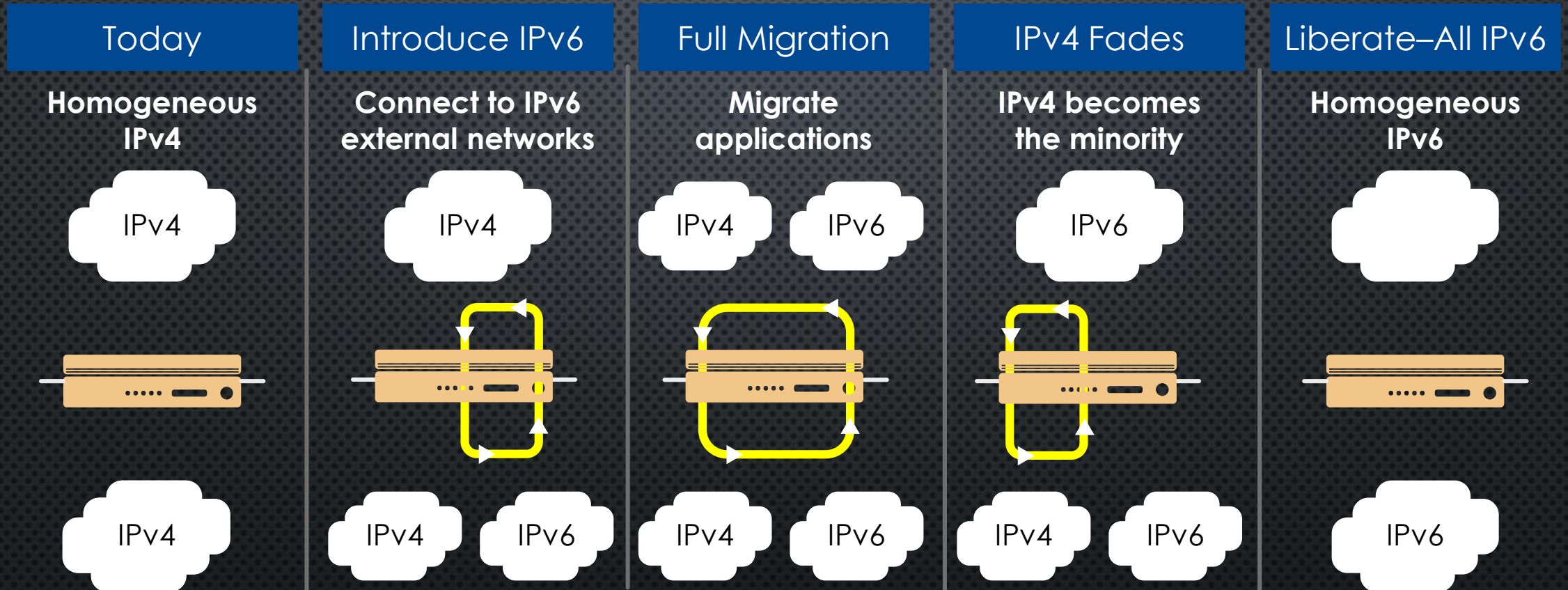
And yes, you could still think about waiting...

Just imagine at the End, if you have a Lifecycle of an application or a Component ahead and you do not migrate.

This will shift the Window of Opportunity to Migrate it to the next migration period or would lead you to a potenital risk to migrate under pressure.
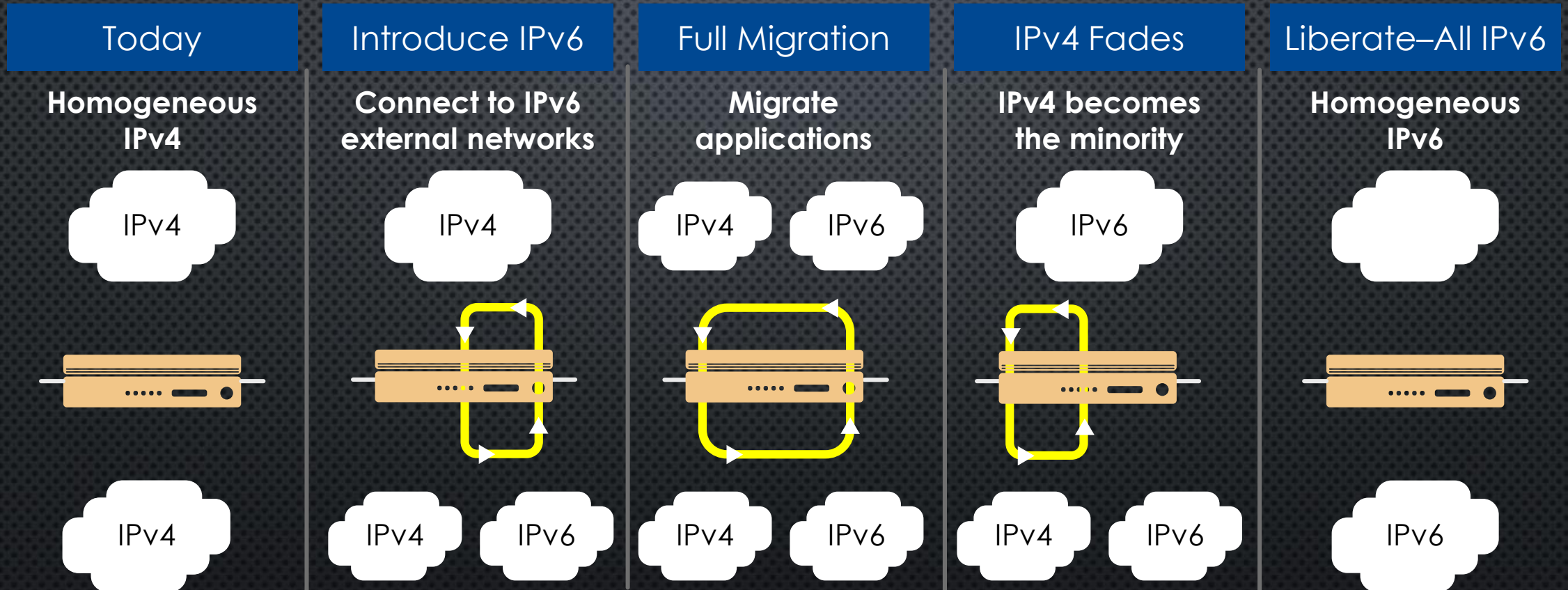
# IPV4 TO IPV6 NETWORK MIGRATION MODEL
## NETWORK MIGRATION AND APPLICATION MIGRATION

| Today | Introduce IPv6 | Full Migration | IPv4 Fades | Liberate–All IPv6 |
|---|---|---|---|---|
| **Homogeneous IPv4** | **Connect to IPv6 external networks** | **Migrate applications** | **IPv4 becomes the minority** | **Homogeneous IPv6** |
| IPv4 | IPv4 | IPv4   IPv6 | IPv6 | IPv6 |
| IPv4 | IPv4   IPv6 | IPv4   IPv6 | IPv4   IPv6 | IPv6 |

Currently, you are probably approaching step 2. and the next step the full Migration is not really moving forward.

# NOT ALL PROBLEMS CAN BE SOLVED JUST.....



...BY BUYING NEW HARDWARE , BUT...

- 8 BLOCKS WITH 4 CHARACTERS SEPARATED WITH ":"
- IN HEX

# IPV4 -> IPV6 CONSIDERATIONS



- Manage the depletion of IPv4 addresses in your network
- Many devices and content will not be IPv6 ready
  - IPv4 and IPv6 are not backwards compatible
- Implement a strategy where both IPv4 and IPv6 co-exist until a complete migration to IPv6
  - IPv4 address management
  - IPv6 migration

# SUMMARY

- Do not be afraid of IPv6

- Pressure will come

- Beeing the Island is no solution

- Do not React, ACT Now

# QUESTIONS ?

Mail: J.Wiesmann@f5.com

Tel: +41 79 454 11 99