
EMSEC: Emanations Security Principle Applied to Networks with IS-IS

Seo Boon NG <sbng@cisco.com>

Agenda

- **What is EMSEC?**
- **Part 1- Customer DMZ Addressing and Advertisement**
- **Part 2 – The Infrastructure Backbone Links**
- **Part 3 – The Loopback Addresses**

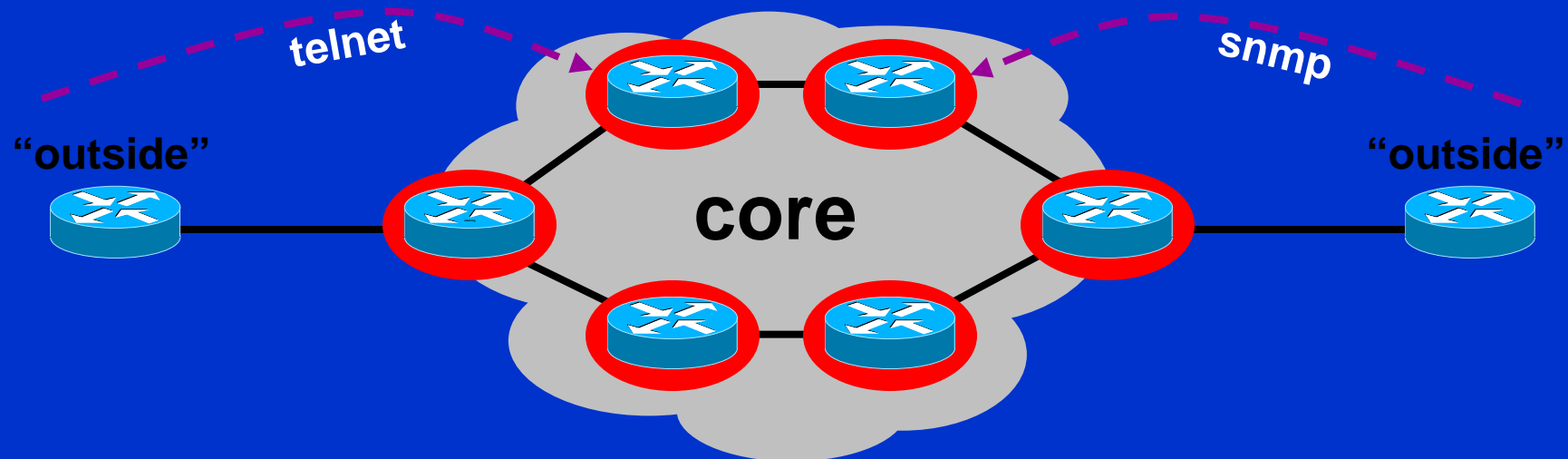
“ **Emanations Security (EMSEC):**
The protection resulting from all
measures designed to deny
unauthorized persons information of
value that might be derived from
intercept and analysis of
compromising emanations from
other than crypto-equipment and
telecommunications systems.”

US Federal Standard 1037C

Is EMSEC *Security through Obfuscation*?

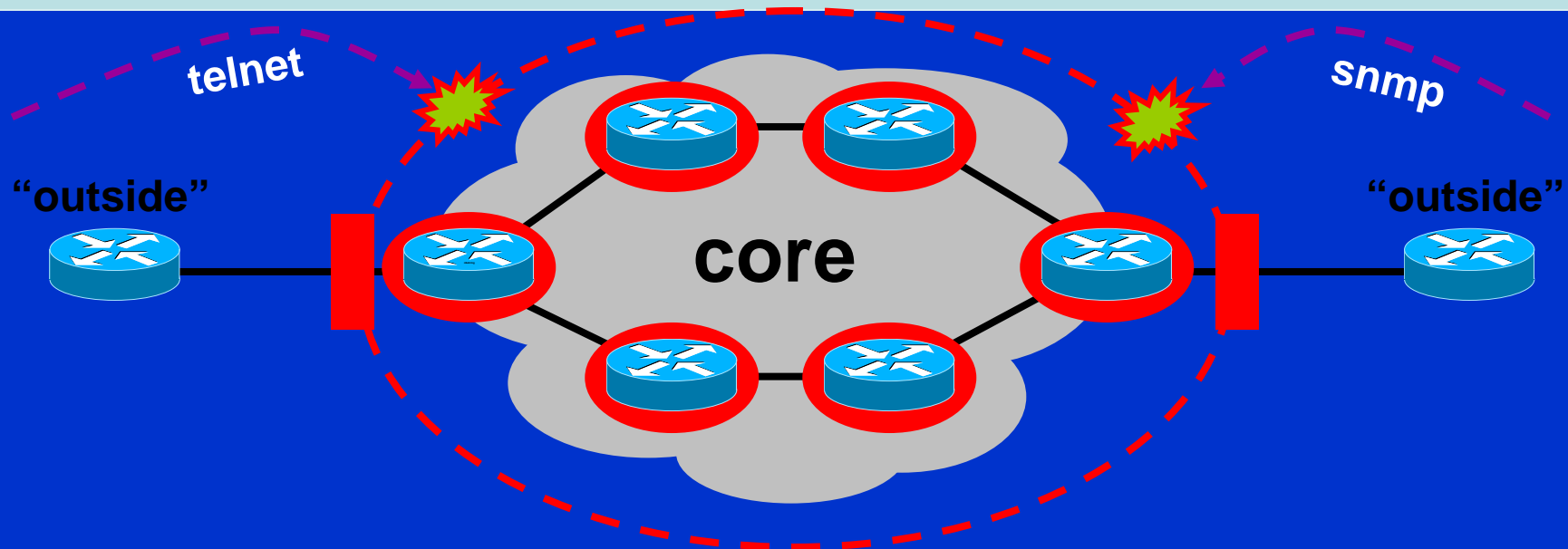
- Security through Obfuscation is hiding and hoping the miscreant does not find me.
- EMSEC principles is denying the enemy intelligence and access to critical command and control elements.
- EMSEC is mindful.
- EMSEC is not the only technique used to secure and harden a system.

The Old World



- Core routers individually secured
- Every router accessible from outside

The New World



- Core routers individually secured PLUS
- Infrastructure protection
- Routers generally NOT accessible from outside

SP Reality Today

- **SP Choose to have little to no EMSEC**
 - **Most if not all infrastructure addresses are advertised to the world**
 - **Most if not all infrastructure addresses have publicly resolvable DNS in-addr records**
 - **Most if not all infrastructure addresses are publicly reachable.**
 - **Addressing is not seen as part of the network security plan.**

Then I'll just use RFC-1918

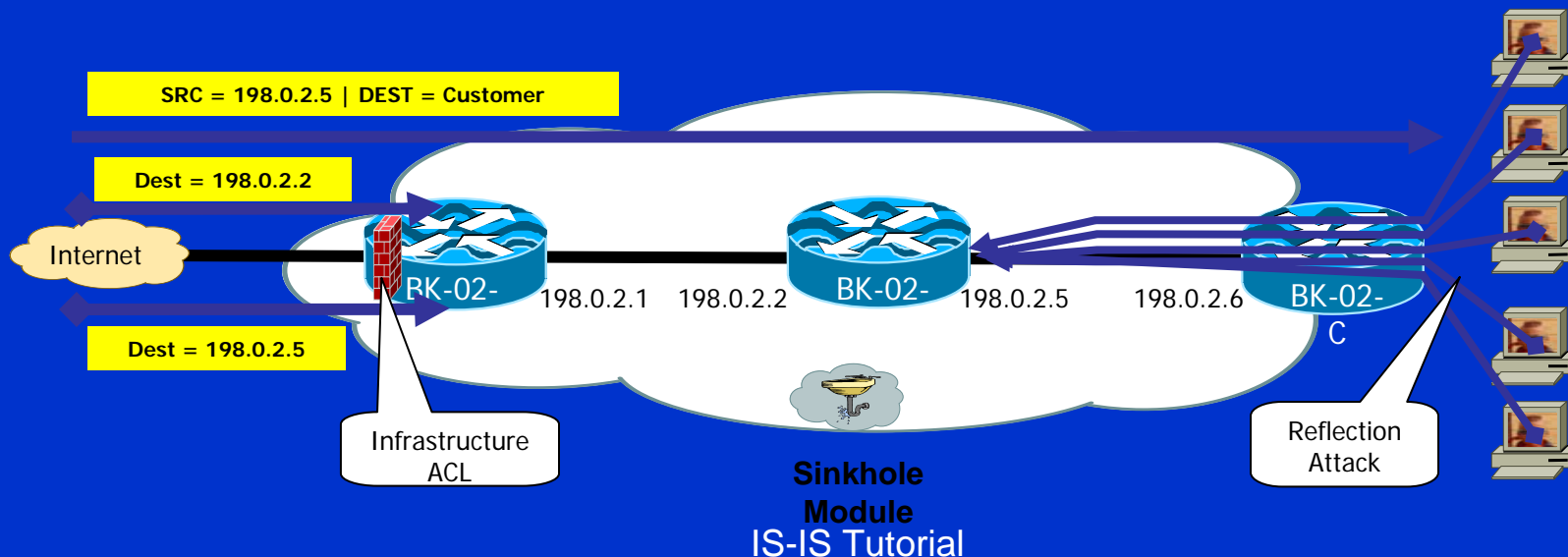
- “Why not use RFC 1918 addresses for all my infrastructure addresses?”
- Operationally, it has proven not to work:
 1. Breaks the guidelines in the RFC
 2. Breaks PMTU
 3. Unexpected interactions with broken customer NATs
 4. Reflection Attacks get around “security through obfuscation.”

Why not iACLs and BCP38?

- EMSEC is works in parallel with other Security Tools in a SP's Security Toolkit.
 - iACLs (Infrastructure ACLs) have an important functions. Yet, *ACL Entropy* but does add to the OPEX.
 - BCP38 does prevent spoofing from your customers, but it does not prevent addresses from arriving to the destination

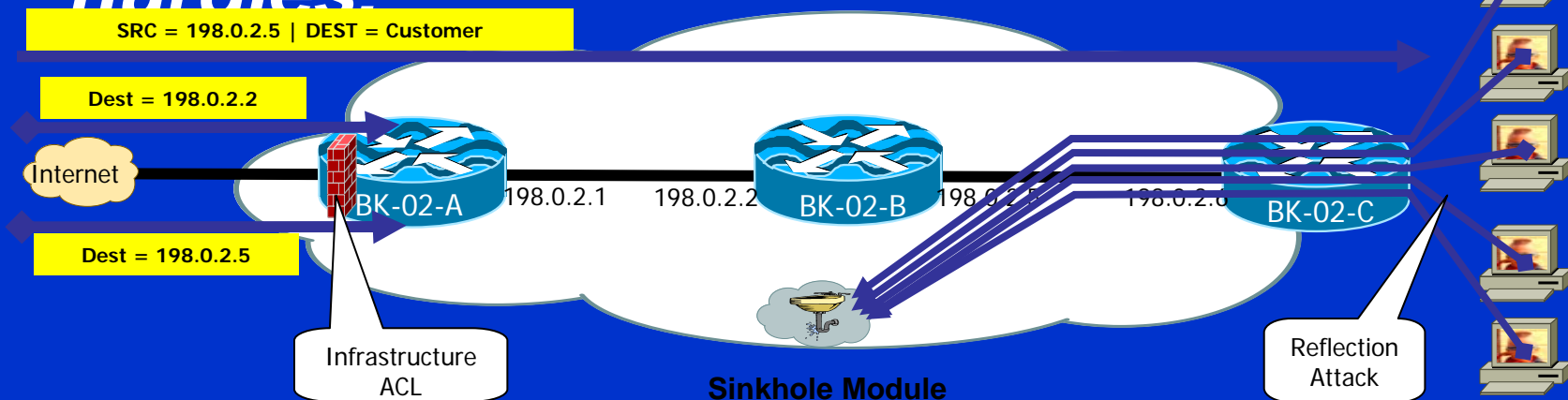
What if I do an ISP Edge ACL?

- Anti-Spoof and Infrastructure ACLs are encouraged on the edge. But
- Need to be everywhere to achieved desired effect – including the customer edge (this is beyond the BCP 38 requirements).



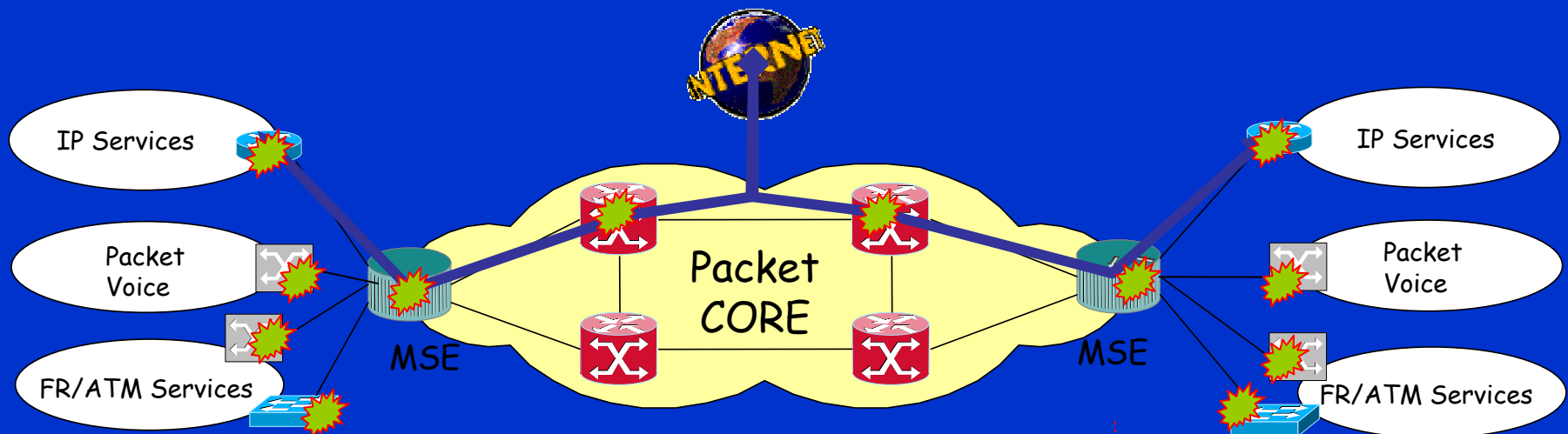
What if I do an ISP Edge ACL?

- Anti-Spoof and Anti-Infrastructure ACLs can be combined with Sink Holing the Infrastructure Blocks.
- Remember – it is all about adding *hurdles*.



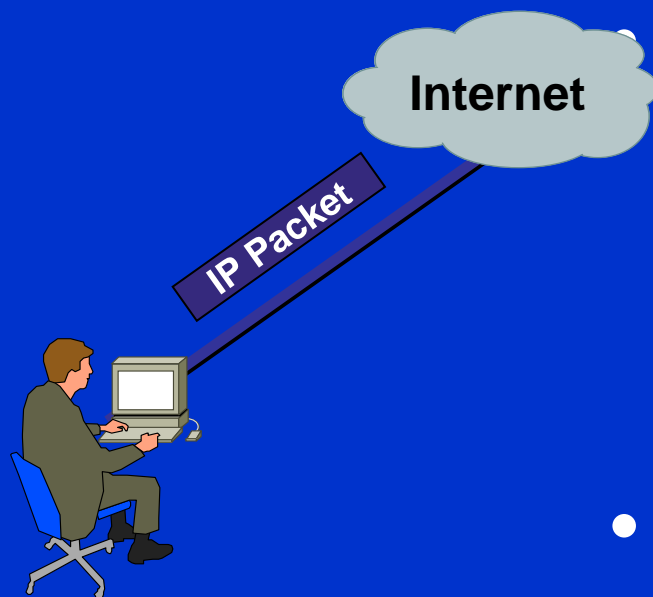
Then I'll just use an MPLS Core

- MPLS Core does work IF you are mindful of EMSEC!
We found lots of MPLS Networks advertising their loopbacks and Infrastructure Blocks!



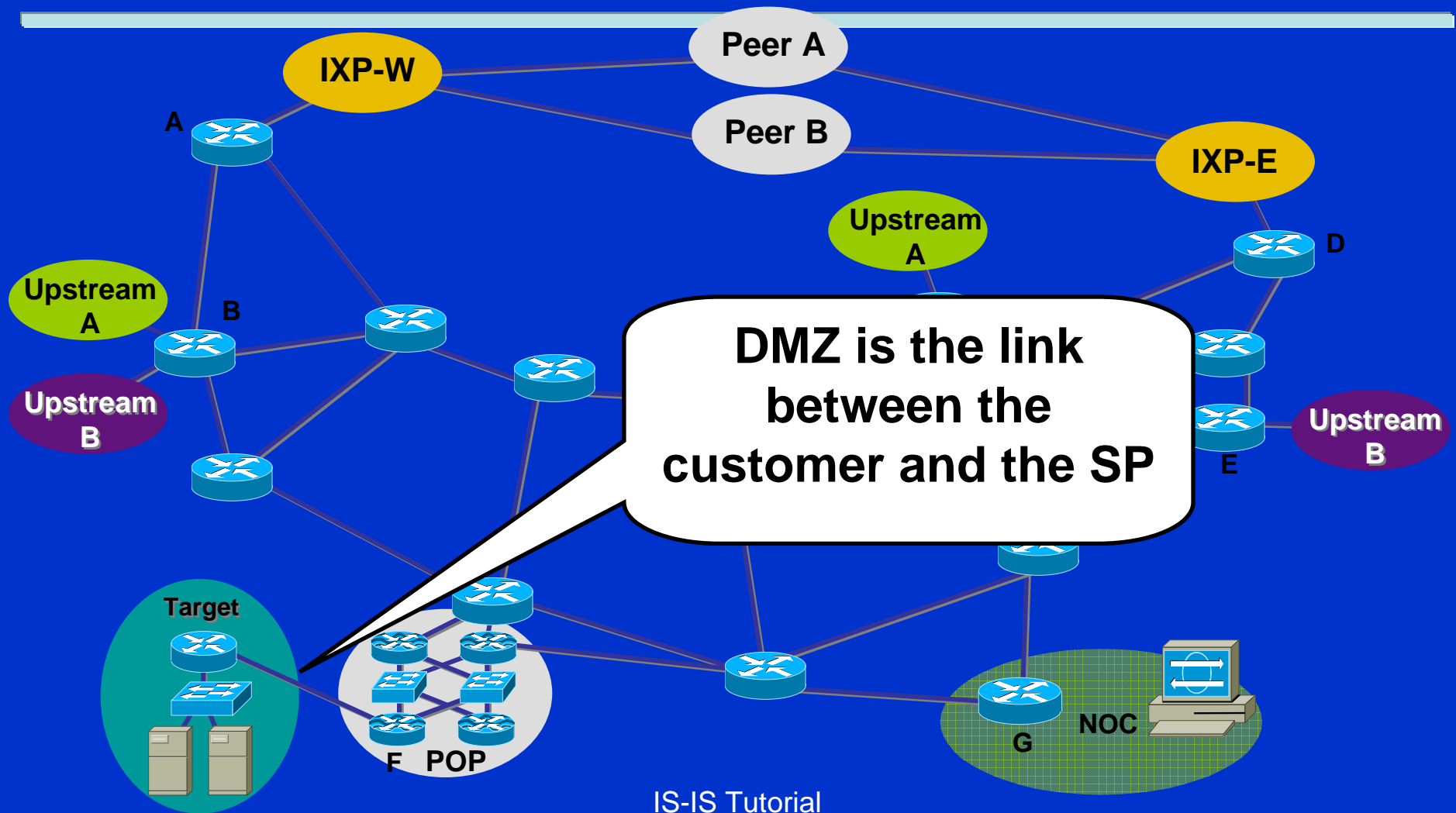
DMZ Addressing and Advertisement

It is all about the packet

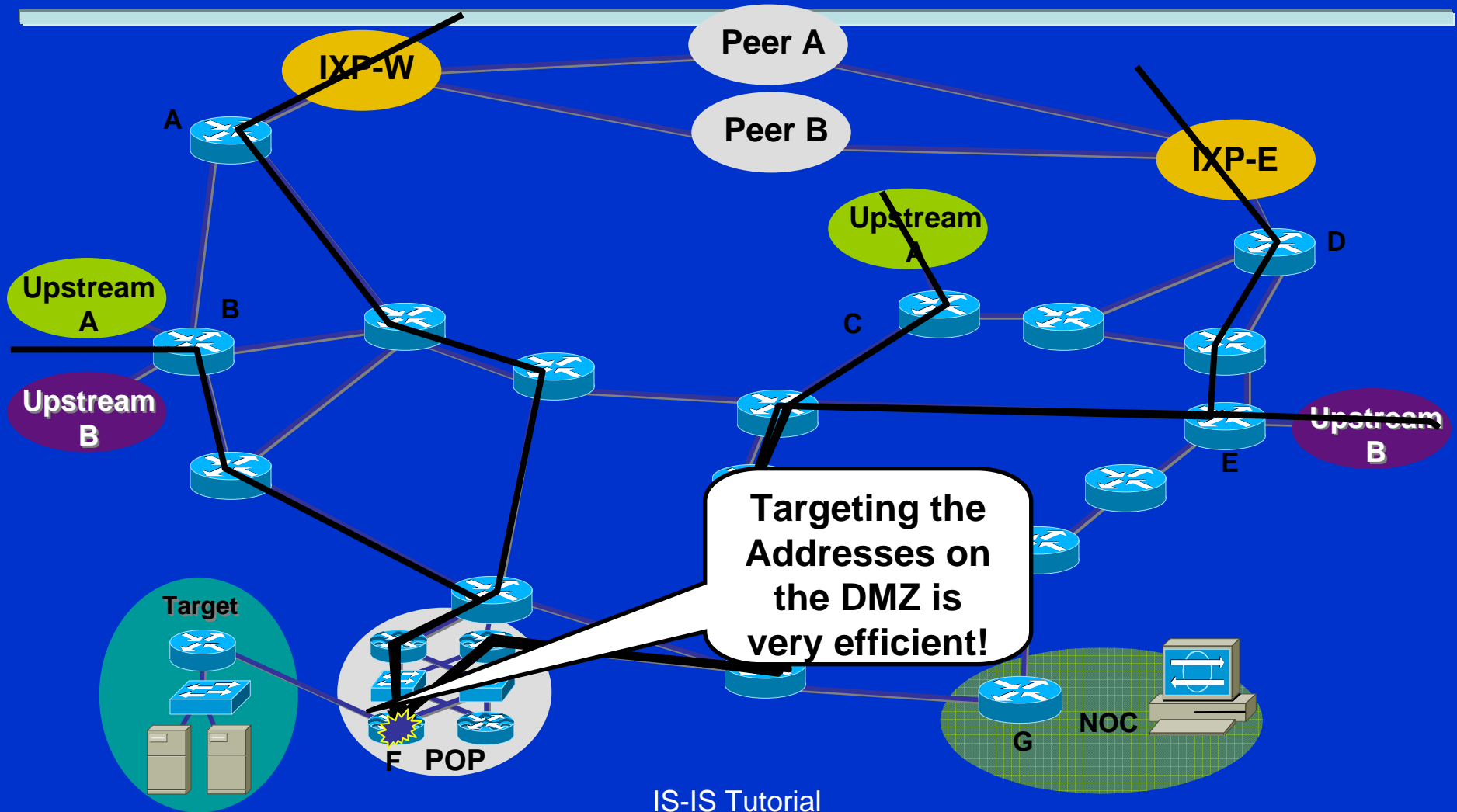


- It is all about the packet
- Once a packet gets into the Internet, someone, somewhere has to do one of two things:
 - *Deliver the Packet*
 - *Drop the Packet*
- In the context of a DOS attack, the question is who and where will that drop that packet.

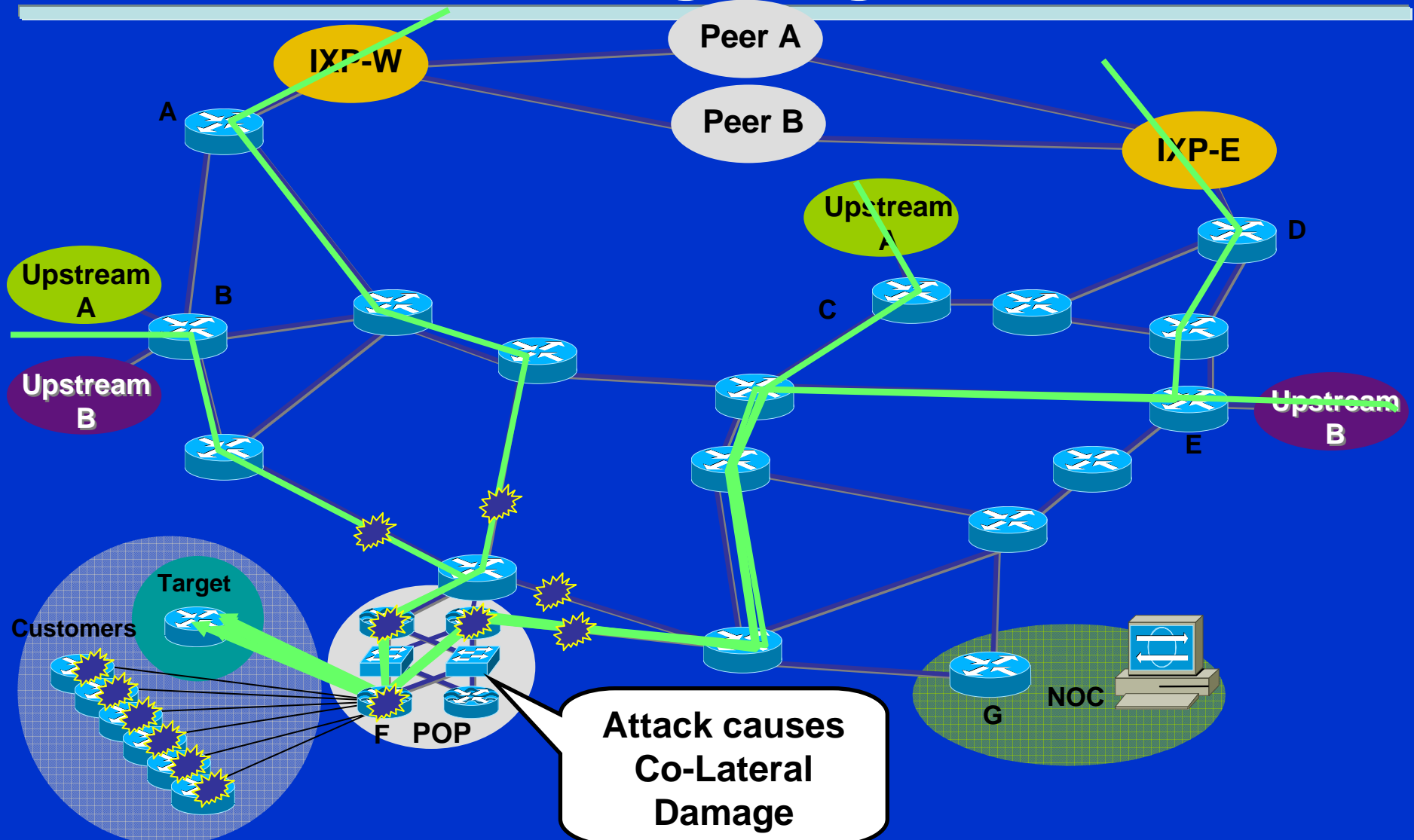
Customer DMS Addresses



Targeting The DMZ Addresses



Co-Lateral Damage from the DMZ Targeting



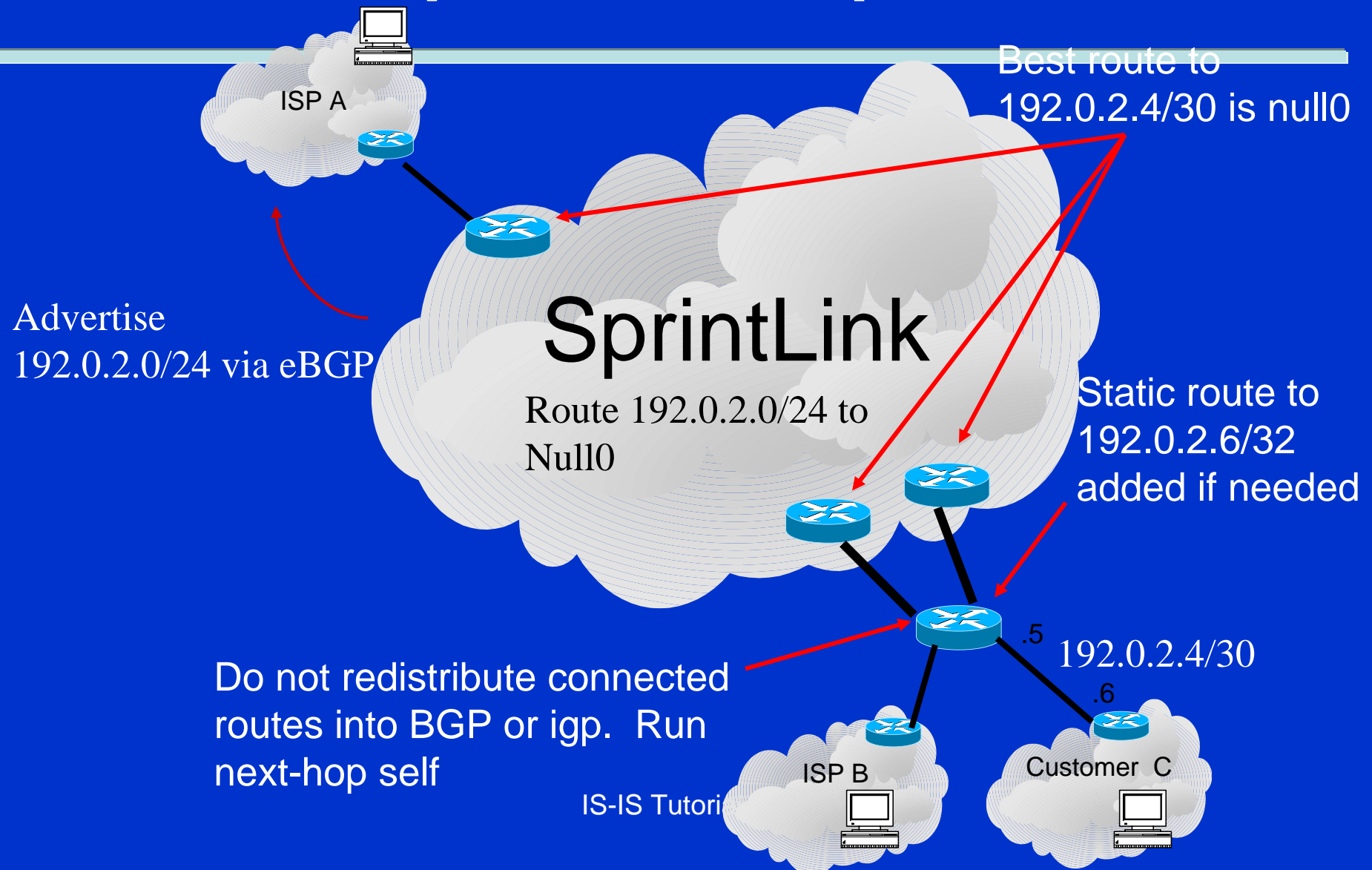
Four ways to number the DMZ Link

- **IP Unnumbered** – Where there is no address on the link.
- **/32** – Where the link is represented as one IP address. Part of the PPP protocol.
- **/30** – Where either side of the link has an IP address. The network and subnet ad
- **/31** – New RFC that saves address space – so that one /30 not becomes two customers vs one customer. Doubles the address utilization capabilities.

Limit Reachability To Customer DMZ IP Addresses

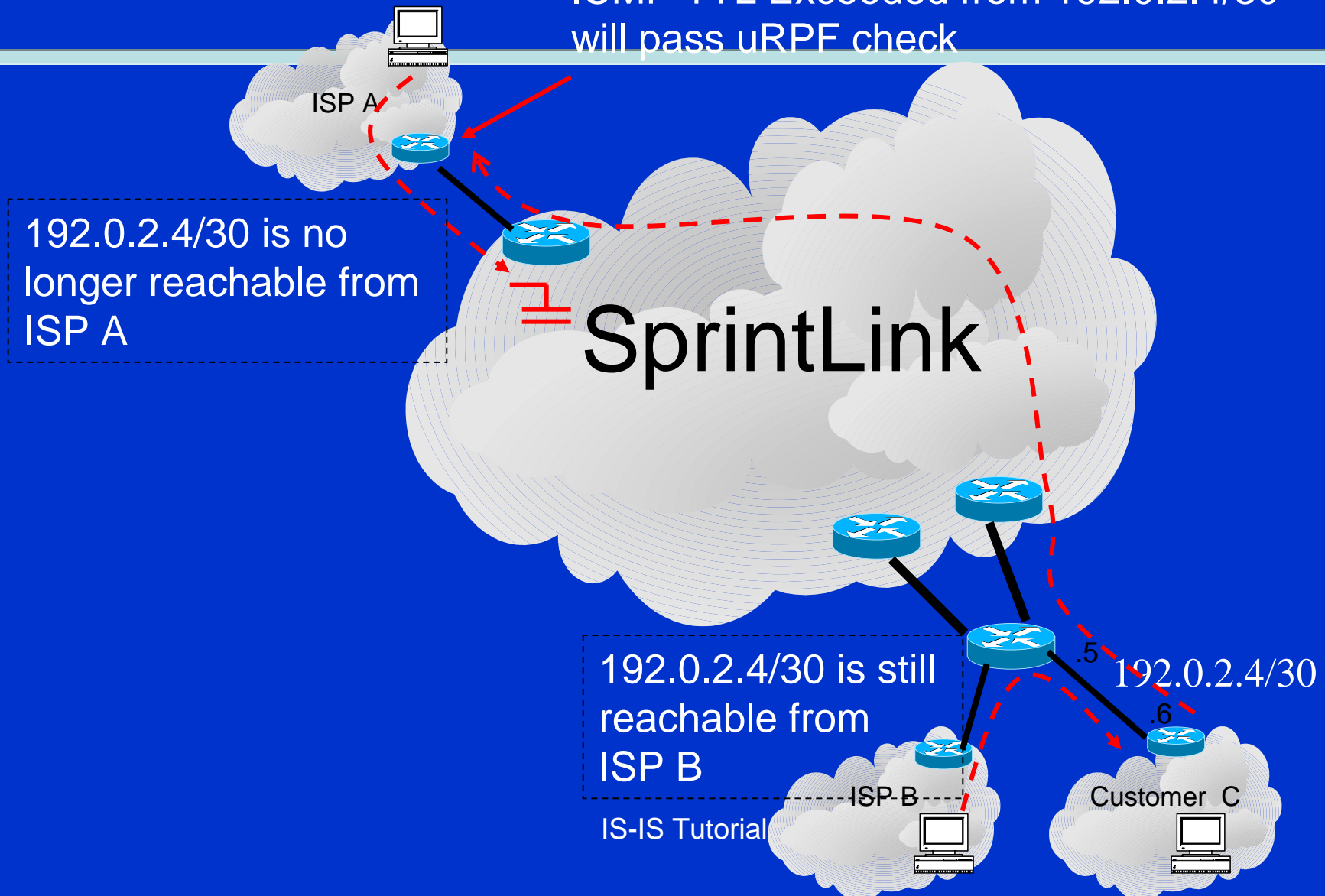
- Most attacks target IP's on routers obtained from a traceroute
- Let's remove the ability to reach Customer's /30 networks from the the big dangerous Internet
 - No one needs to reach the /30 besides the adjacent routers
 - Stop redistributing connected-routes into BGP
 - Continue to advertise /16 aggregates to the world
 - Best route becomes the /16 to null0 on the rest of the network

Sprint's Example



Sprint's Example

ICMP TTL Exceeded from 192.0.2.4/30
will pass uRPF check



Limit Reachability To Control Plane IP Addresses

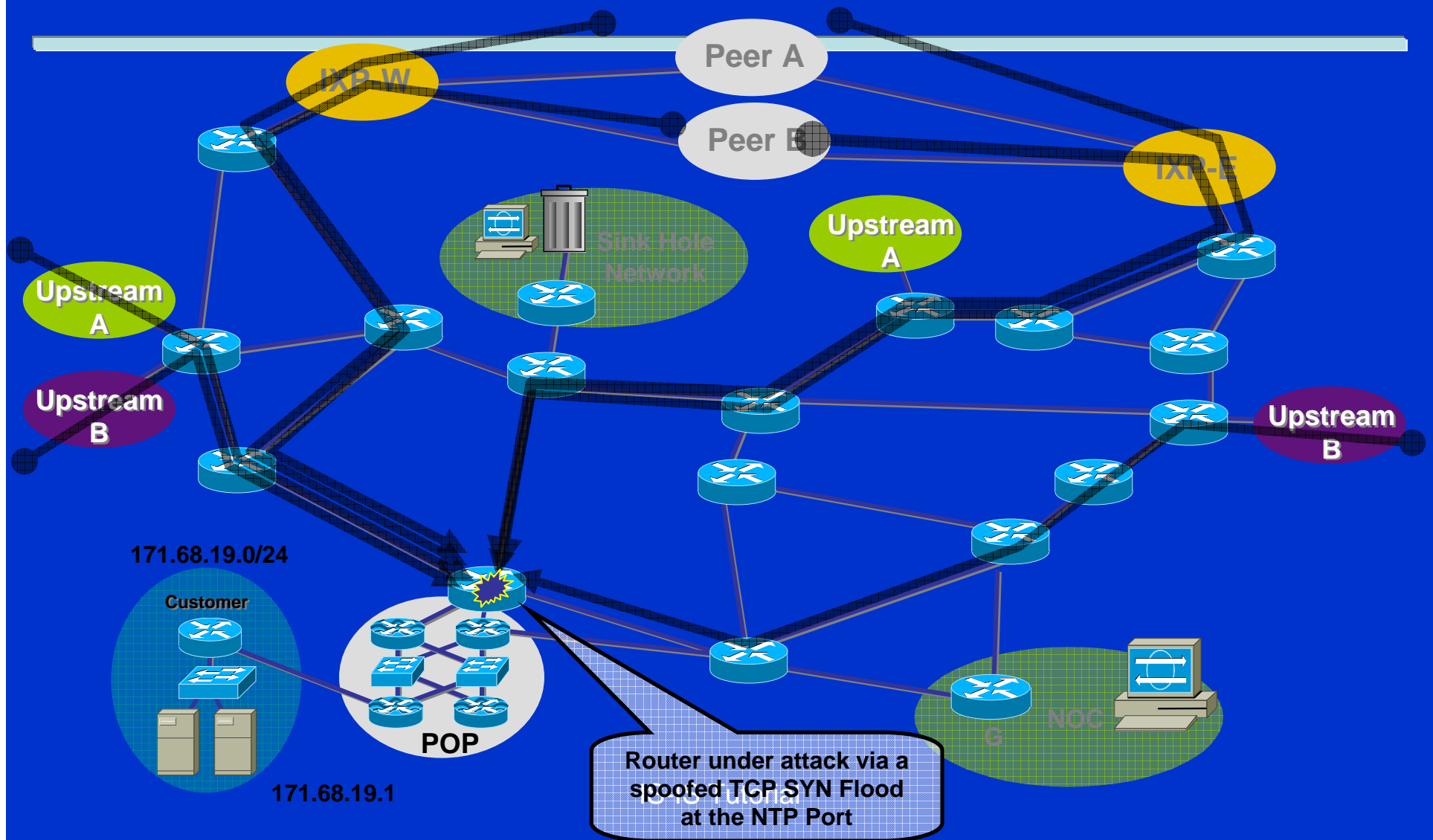
- **Does not add 100% security**
 - But, makes it a little harder for the attacker
- **Implications**
 - Traceroute through the router not impacted
 - Any packets to the routers breaks
 - PING
 - Folks LOVE to PING our routers...
 - Traceroute

What next?

- Do the same thing in the core
 - Utilize Cisco IS-IS enhancement
 - “advertise-passive-only”

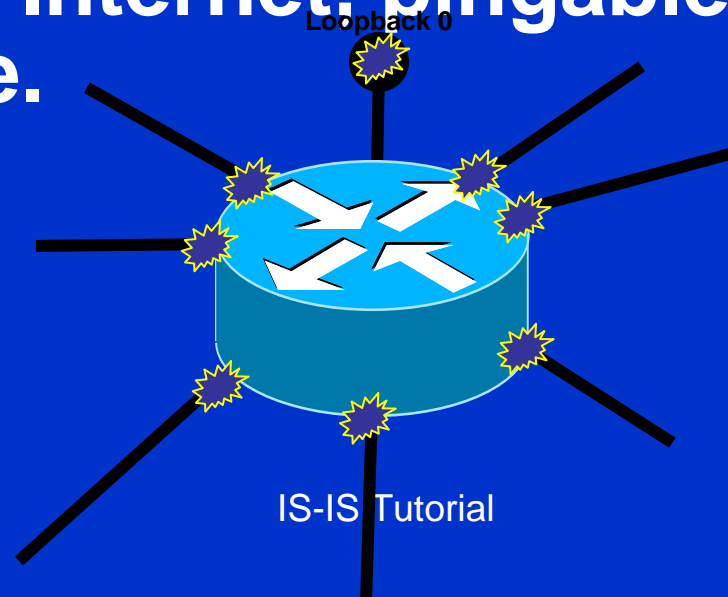
The Infrastructure Backbone Links

Routers do get Directly Attacked



Today's Principle - Reachability

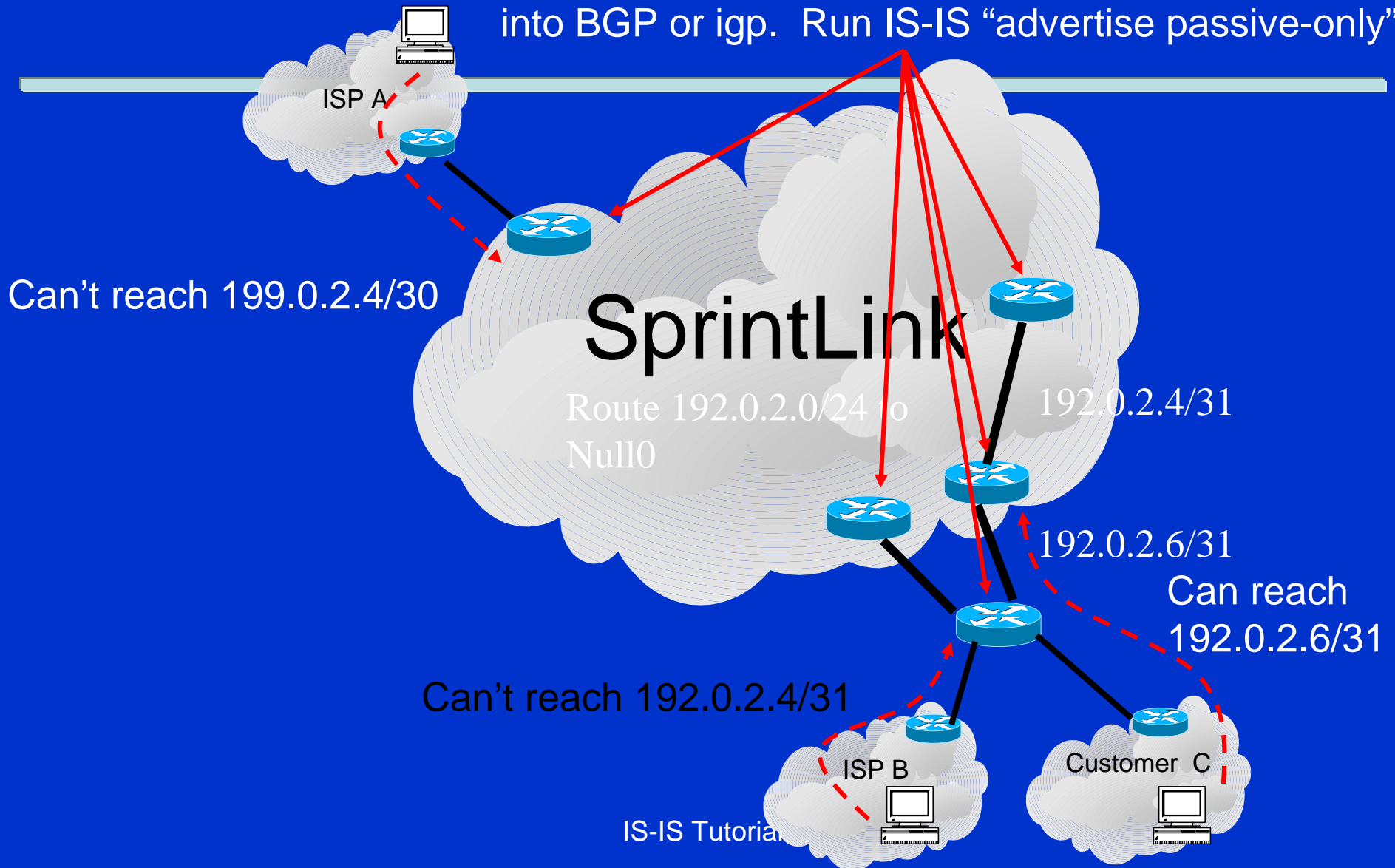
- Today, the BCP is to insure there is reachability to all the links going into a device on the backbone.
- Links are usually /30s – reachable from the entire Internet, pingable, and targetable.



Sprint Example

APRICOT
PERTH 2006

Do not redistribute connected routes into BGP or igp. Run IS-IS “advertise passive-only”



What next?

- **Do the same thing in the core.**
 - **Utilize Cisco IS-IS enhancement**
 - “advertise-passive-only”
- **Ignore IP-Options**
 - **Forward packets as if there was no options set**

Loopback Addresses

Loopback Address Reachability

- The only ones who need access to the loopback addresses are the owners of the Autonomous System.
- Hence, you do not need to advertise the loopback addresses out of the SP
 - Can use RFC 1918 Private Address Space
 - Use iACLs on the edge
 - Use uRPF Phase 3 (if we ever finish it)
 - Put them into a separate VRF

What does all this mean?

- **Don't plan on sending any packets destined to the router.**
 - But this is already happening with the MPLSization of networks.
- **More secure infrastructure**
 - Not perfect, but better than where most of us are now.

The SP EMSEC Story

- **Information access**
- **Customer DMZ Addressing and Advertisement**
- **The Infrastructure Backbone Links**
- **Loopback Addresses and Advertisement**
- **DNS Infrastructure Addresses**
- **Services Infrastructure Addresses**

Summary...

- IS-IS fast convergence enhancements improve security...
- You can't route (directly) to IP addresses that aren't in the routing table!
- iBGP is tied to the routers loopback interface. Hence, the IP addresses of the individual infrastructure links are not required and can be removed from IS-IS
 - Use the global IS-IS configuration command `advertise passive-only` to remove all interface IP addresses from the IS-IS database
- Packets with a source IP address of a infrastructure link can cause a "reflection" attack to reach that infrastructure address.
 - uRPF strict mode can mitigate this type of attack