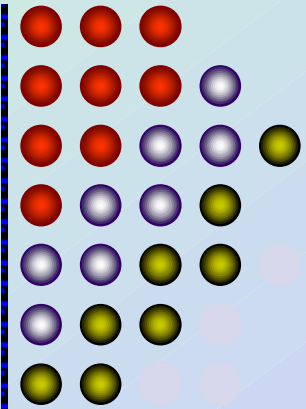


# **\$tealing with BGP**

---



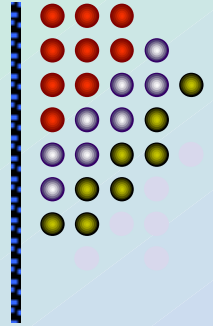
**By**

**Stephen Dugan, CCSI**

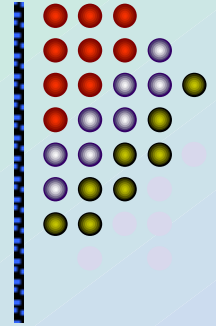
**[scdugan@101labs.com](mailto:scdugan@101labs.com)**

# Topics for today

- Who Cares about BGP?
- BGP Basics
- Major BGP Flaws
- Redirecting Traffic
- Solutions with S-BGP
- Q & A

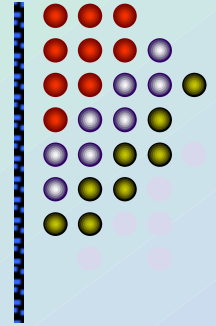


# Who Cares about BGP?



- At the core of the Internet's operation is the Border Gateway Protocol (and Caffeine)
- ISPs use BGP to exchange reachability information.
- Think of it as a very complex version of RIP
- Built upon the assumption of trust
- The current version is BGPv4, and was drawn up on a napkin

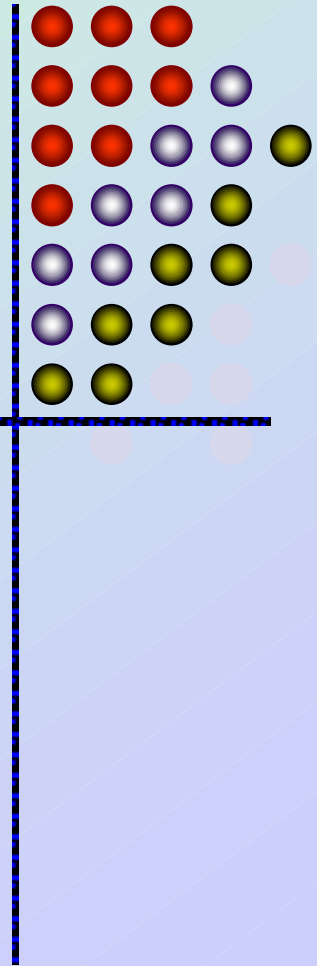
# Who Cares about BGP?



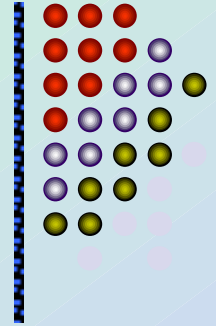
- ADoS (Administrative Denial of Service) mistakes are common (AKA opps!)
- Malicious DoS attacks could greatly disrupt or stop traffic
- DoS and ADoS attacks can have global impact
- Securing the existing BGP implementation is taking too long!
- Basic MD5 security is often not implemented

# BGP Basics

---

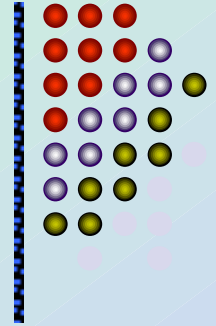


# BGP Terms



- **Prefix:** An IP subnet, network, or aggregate of networks representing a single entry in the BGP Routing Table
- **Autonomous System:** Domain of administrative authority
- **Autonomous System Number:** 2 byte value for identifying an AS (0-65535)
- **AS path:** Numbered “Hop-Count” listing the order ASes needed to traverse back to the owner of the advertised network.

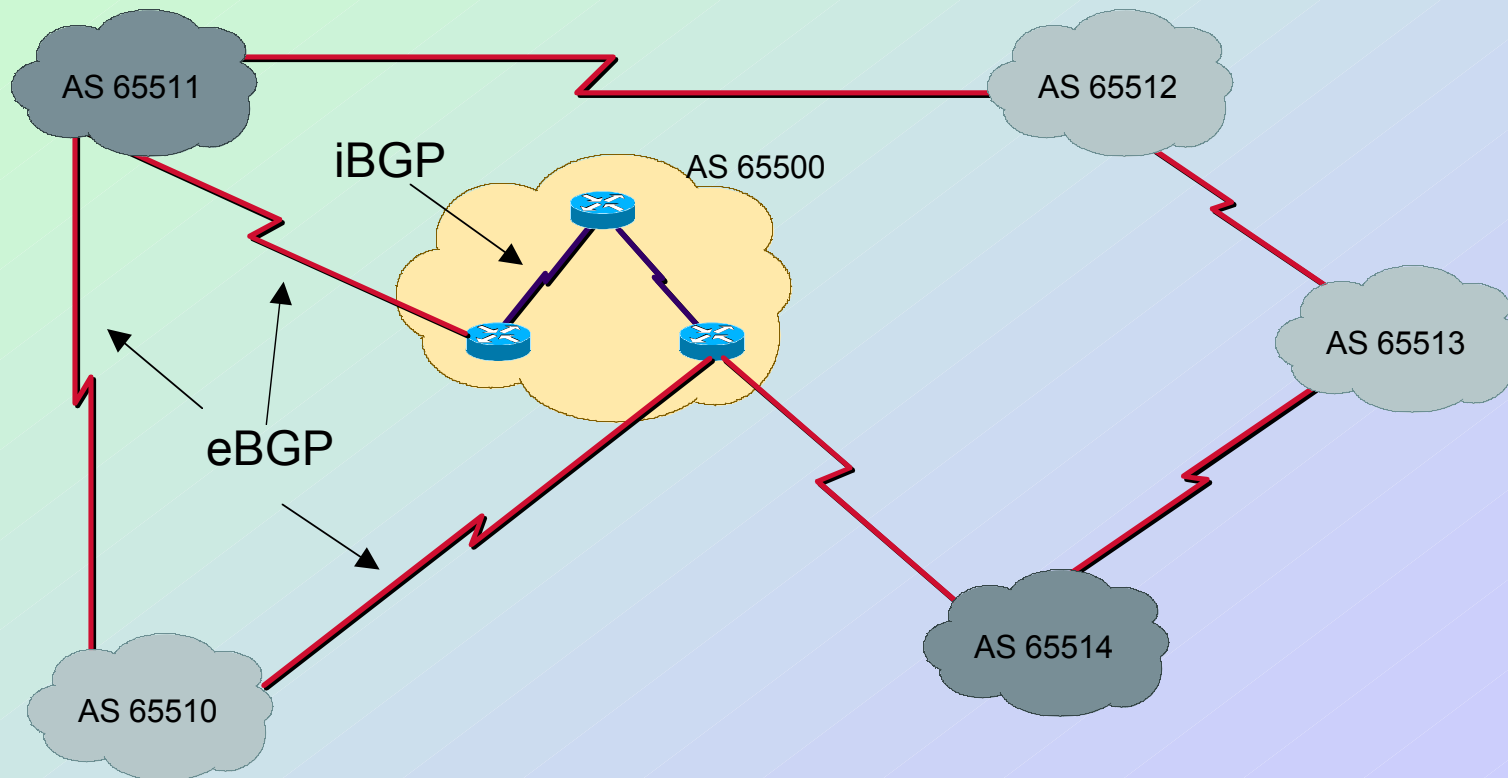
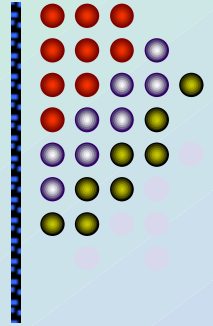
# BGP Size (Today)



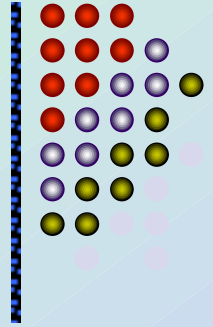
- Nearly 12,000 routers are currently running BGP (Not all have the full RIB)
- The RIB shows 6,500 AS numbers, although almost twice that have been assigned.
- Close to 130,000 listed prefixes
- This equates to around 18,000 paths
- Most routes are 3-4 AS hops, less than 5% are greater than 5 ASes

# BGP “anti-hierarchy”

BGPv4 doesn't have any controlled Hierarchy like OSPF or ISIS



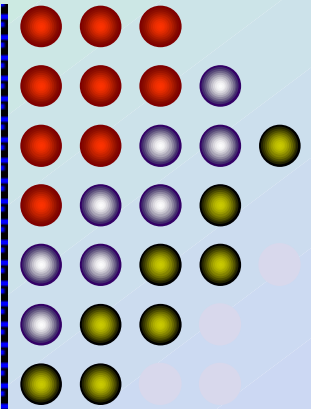




# BGP Updates

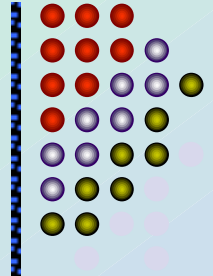
- BGP is not used to forward end-User traffic, but rather to create the paths for this traffic to follow
- BGP changes are sent via a BGP UPDATE messages
- BGP uses the UPDATE information to determine the “best path” to a prefix
- “Best Paths” can be controlled within an AS and may not be the shortest “Hop-Count”

# Major BGP Flaws

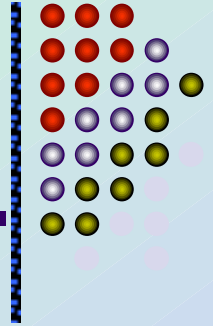


# An “ASS” of “U” and “ME”

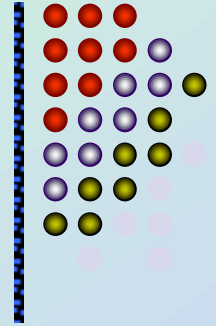
- An AS is responsible to only advertise or withdraw prefixes to which they have been assigned
- When receiving an UPDATE you must assume that your neighbor (or your neighbors neighbor) has authority to advertise a network
- It is appropriate to establish filters to make sure your neighboring ASes only advertise networks assigned to them



# An “ASS” of “U” and “ME” cont.

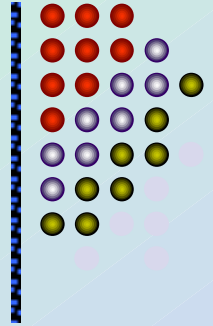


- Within an AS path, the first listed AS is the advertising (or originating) AS
- You must assume that your neighbor hasn't incorrectly modified the AS path attribute
- It is because of these assumptions that BGP is vulnerable to the possibilities of route manipulation, black holes, local and global DoS, wiretapping and server masquerading



# BGP is a Global Problem

- ALL BGP routers are vulnerable
  - Implementation flaws
  - Manufacture OS bugs
  - Authorized or unauthorized Physical Access
- A compromised BGP router can be used to attack resources in other ASes
- Many of these attacks cannot be mitigated by any of our existing local security solutions

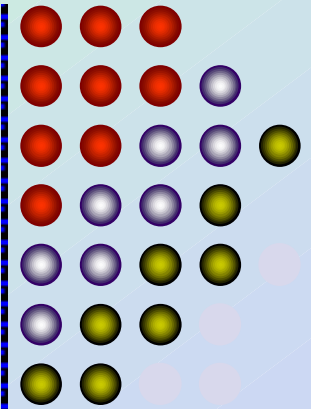


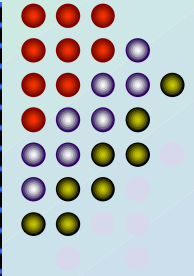
# Filtering is ineffective

- The only protection is for ISPs create filters and local policies to guard against malicious or accidental errors
- These filters and policies are time consuming, difficult to create and maintain, and highly subject to error
- One “Owned” router can often ignore or modify local and AS level policies
- Management stations controlling BGP policy are also subject to attacks

# Redirecting Traffic

---

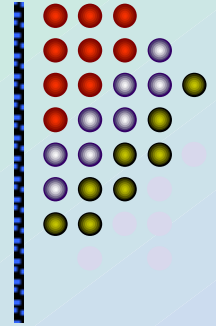




# Why Attack BGP?

- Several types of DoS attacks with varying levels of impact
  - Single network
  - Multiple Prefixes
  - Single AS and/or neighboring ASes
  - Network Access Points (NAP)
  - Global Level attack
- DDoS attacks have yet to take full advantage of the existing BGP vulnerabilities

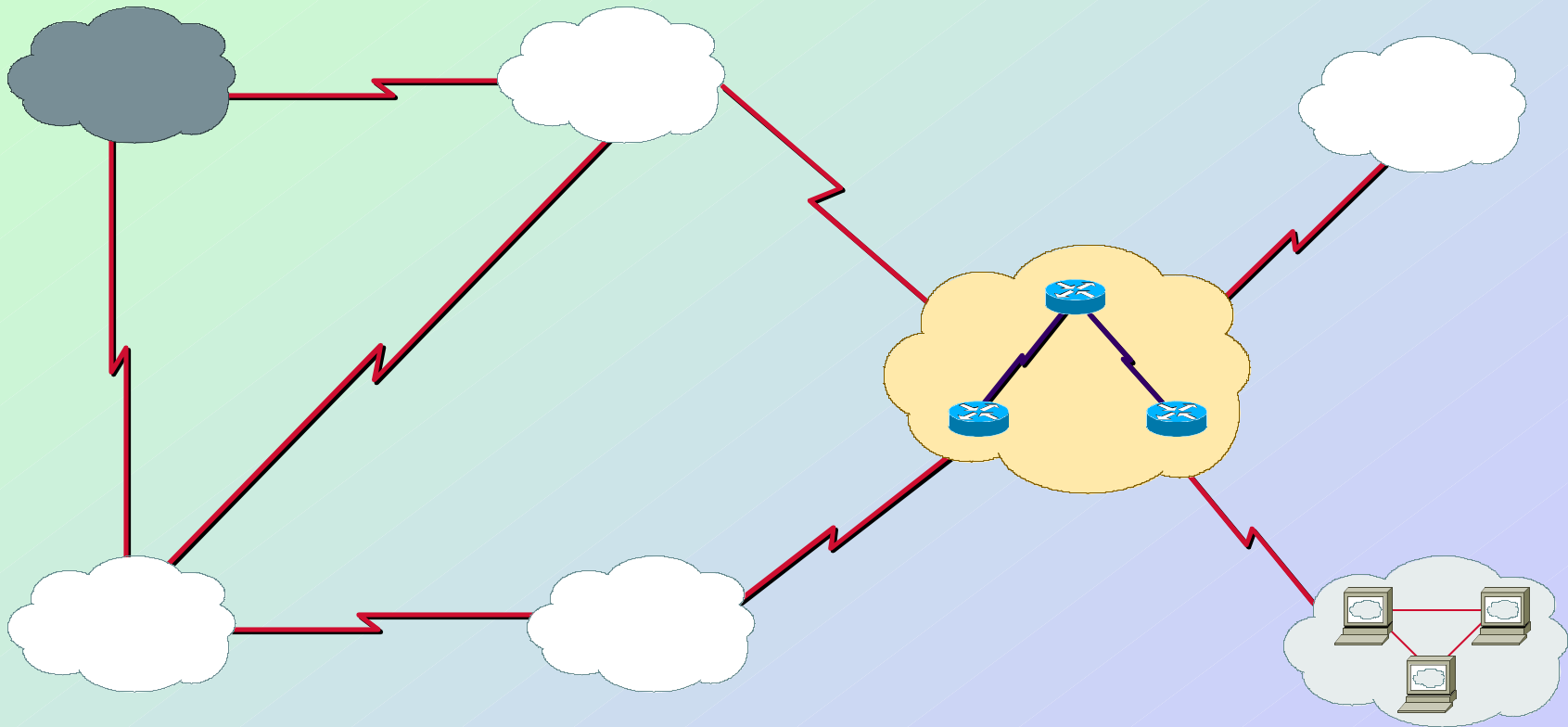
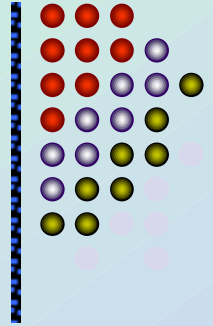




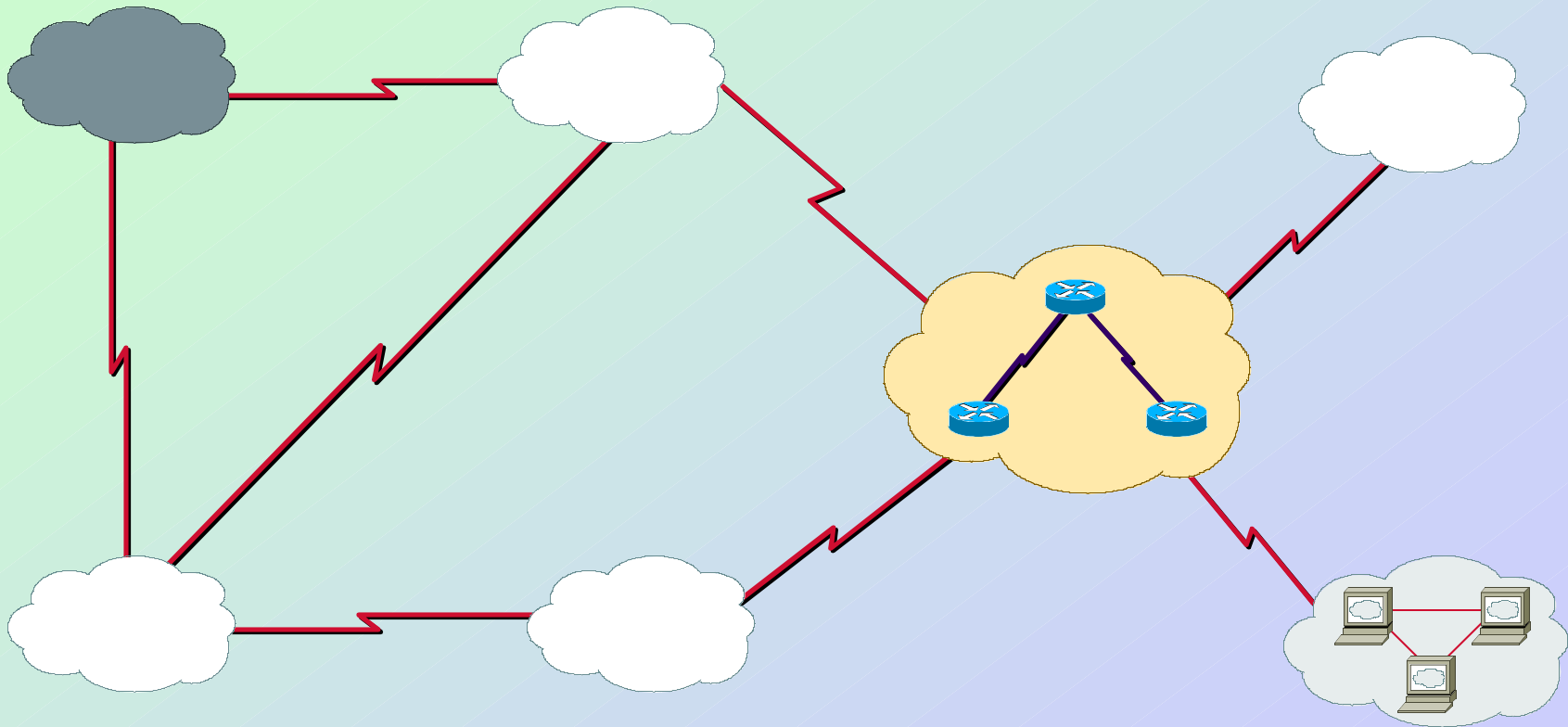
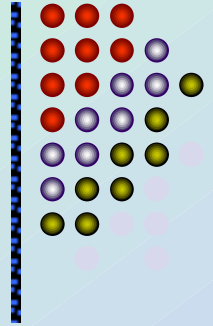
# Why Attack BGP? (Cont.)

- Redirect traffic
  - Wiretap / Man-in-the-Middle
  - Manipulate end user traffic
  - Create a “Blackhole”
  - Session Hijacking
- Server Masquerading
  - Become the Bank (\$tea£)
  - Backdoor files to be downloaded
  - Deface websites

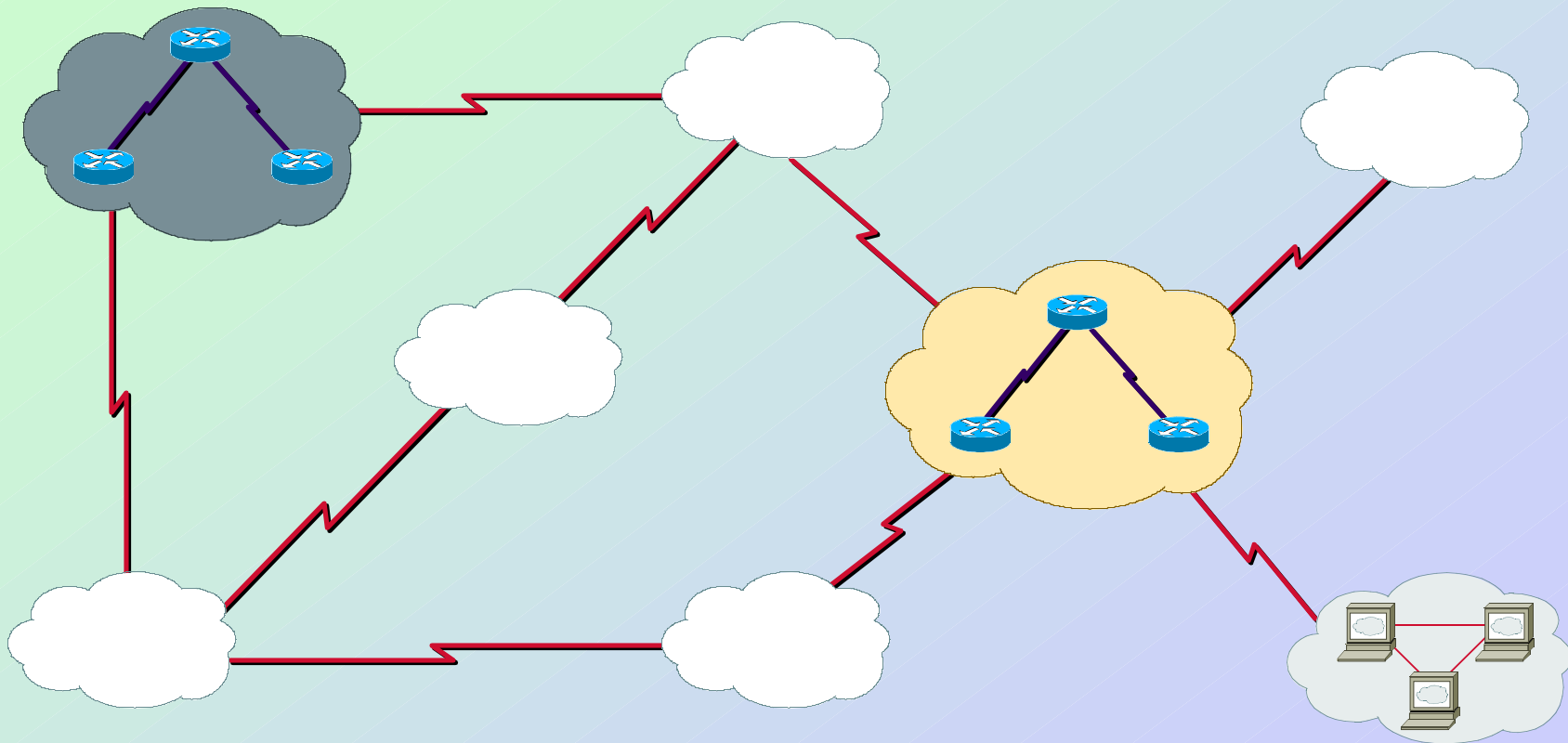
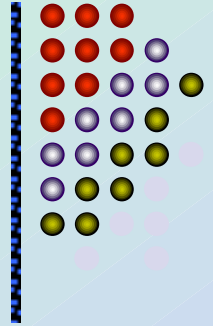
# BGP DoS Attacks



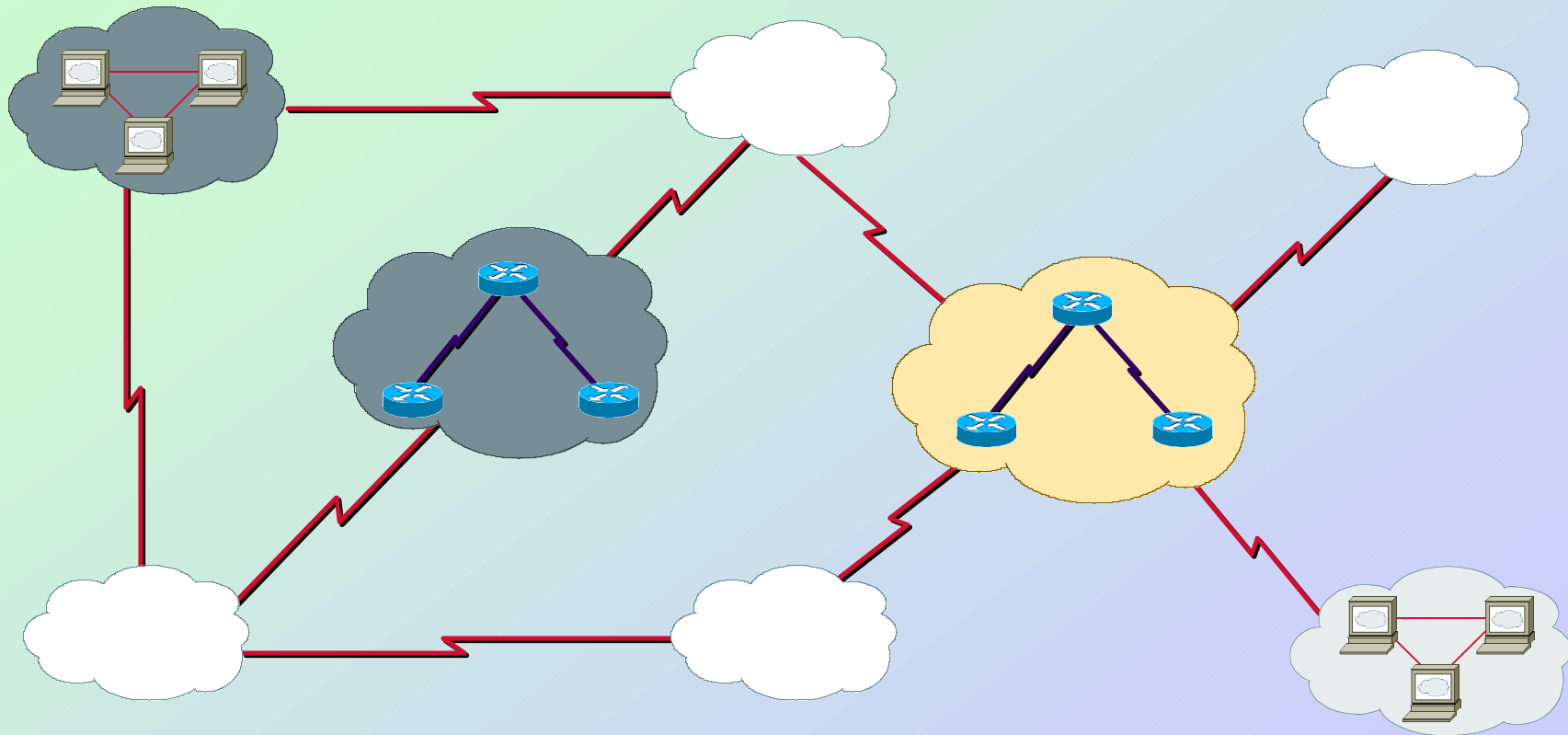
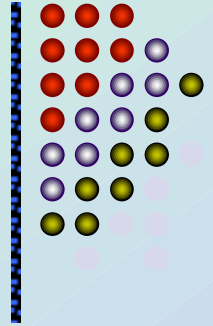
# BGP DoS Attacks 2



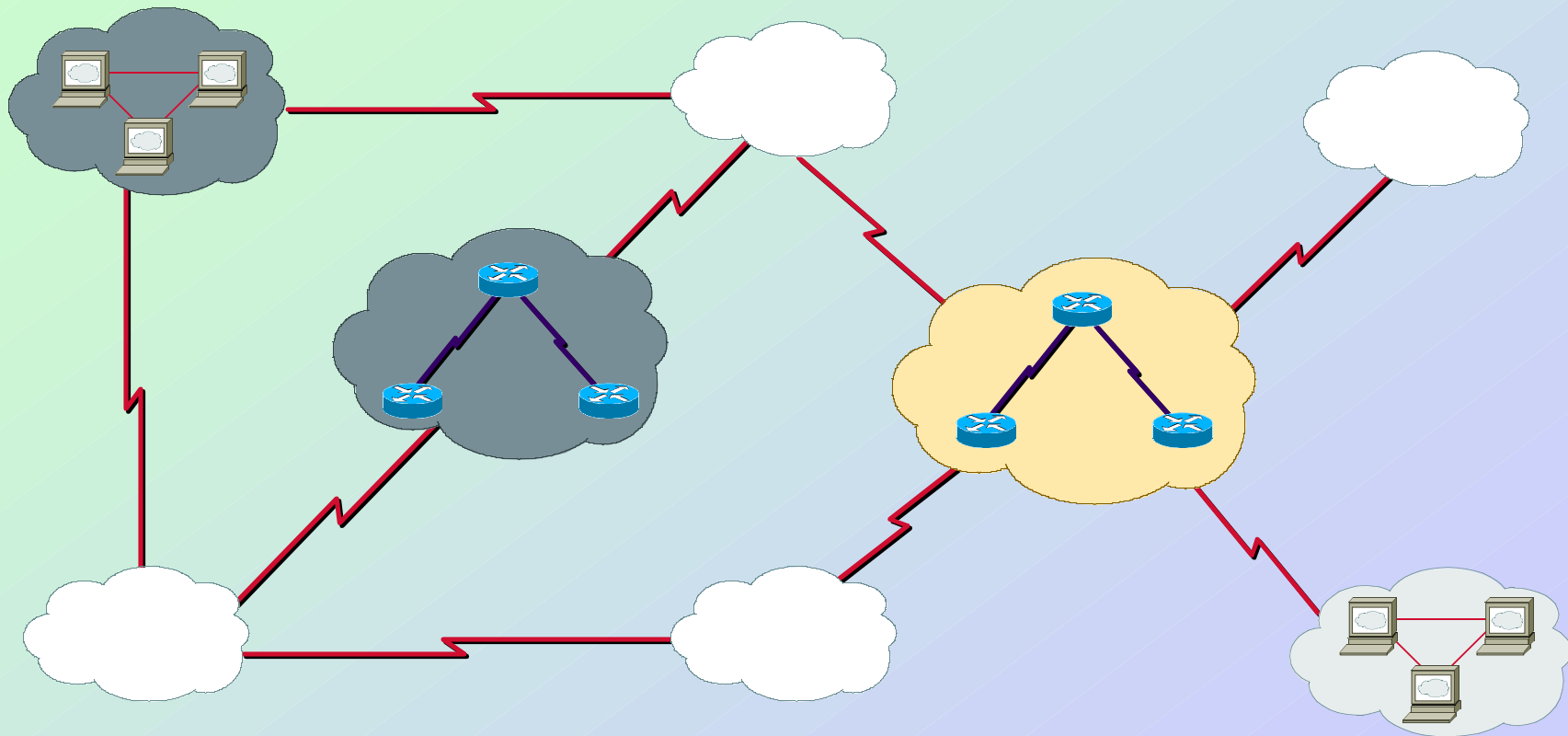
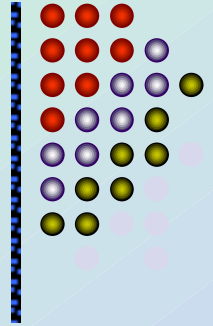
# BGP Redirection (Blackhole)



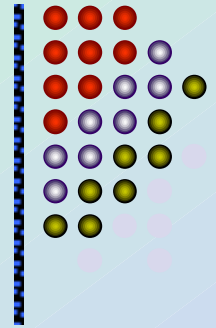
# BGP Redirection (Wiretap)



# BGP Redirection (Masquerade)



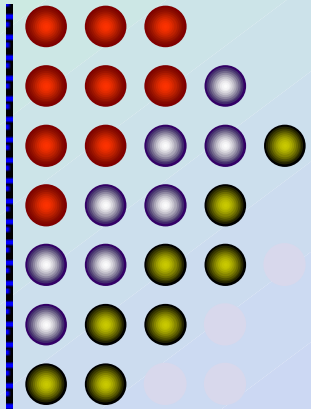
# What's happening Today?



- Configuration errors (not specifically attacks) affect about 1% of all routing table entries at any time
- Tools targeting BGP have been written and demonstrated and shows like BlackHat
- Remote Route injection is theoretically possible (Weak ISN, existing bugs) and rumors of tools existing within private circles
- ANY router flaw causing a Crash against a BGP router could have a wide spread effect

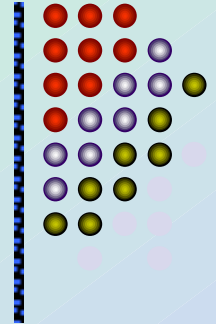
# Solutions with S-BGP

---



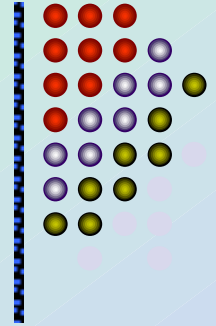


# S-BGP Requirements



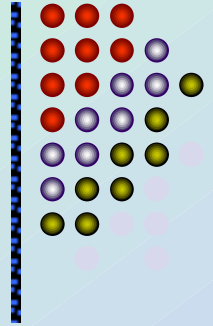
- Stop Trusting other ASes
  - What if you fire an employee that goes to work for a neighboring AS?
  - Do you trust ISP dedicated to SPAM and questionable content
  - Small ISPs have the same vulnerabilities with less resources to secure their routers
- BGP traffic needs protection from evesdropping and possible manipulation (IPSEC)

# S-BGP Requirements

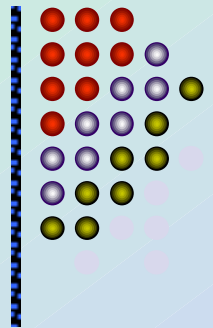


- The Origin and Path must be verified
  - Is the last AS in the AS-PATH really the network Origin? (Prove it!)
  - Prefix/AS matching with PKI
  - Does every AS in the AS-Path have the right to advertise this Prefix?
  - Verification of add/withdrawal UPDATE messages

# S-BGP Requirements Cont.



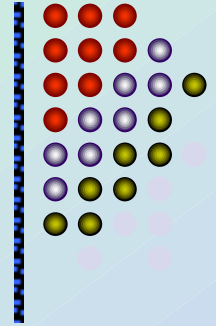
- Must Fully integrate with BGPv4
  - We cannot expect all of the ISP of the world to implement this at once
- S-BGP should not allow for IGP and Static routing to circumvent security
- Should also carry Bogon routes (From RIPE, ARIN, ect.) as a form of Dynamic filtering
  - Traffic sourced from Bogons still account for a tremendous amount of global traffic



# Main S-BGP Issues

- S-BGP has a significant cost to its implementation
  - Costs include
    - S-BPG software development
    - Interoperability testing
    - Route Registries issuing CAs
    - Router upgrades (RAM / NVRAM / CPU)
    - Staff training
- Deployment
  - The advantages of S-BGP cannot be realized until a majority of ISP are up and running
  - Many are not still convinced of the need for S-BGP
    - Are we all just waiting for the first REAL BGP attack?

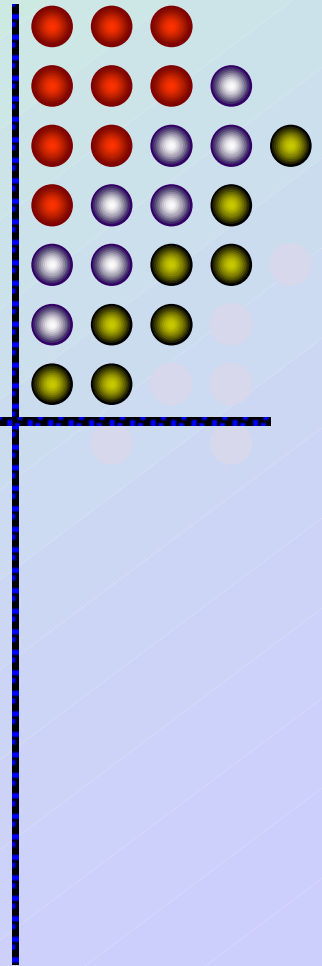
# Summary



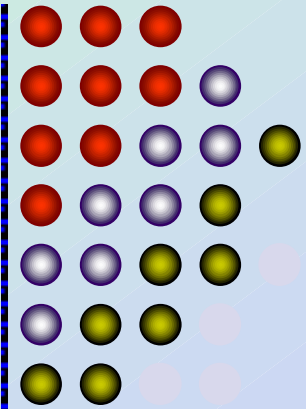
- BGP is an Important, Critical and vulnerable part of the Internet
- BGP Attacks are going to get worse
- With a problem of this magnitude we must all strive for a solution, NOW!
- Trust only goes so far.... How soon until that trust is shattered?

# Q & A

---



# Thank you for coming!!



Special thanks to

Jeff & Ping, kM, SPuD, and the rest of  
the Black Hat Crew

ROUTER

ALL YOUR ~~BASE~~ ARE BELONG TO US