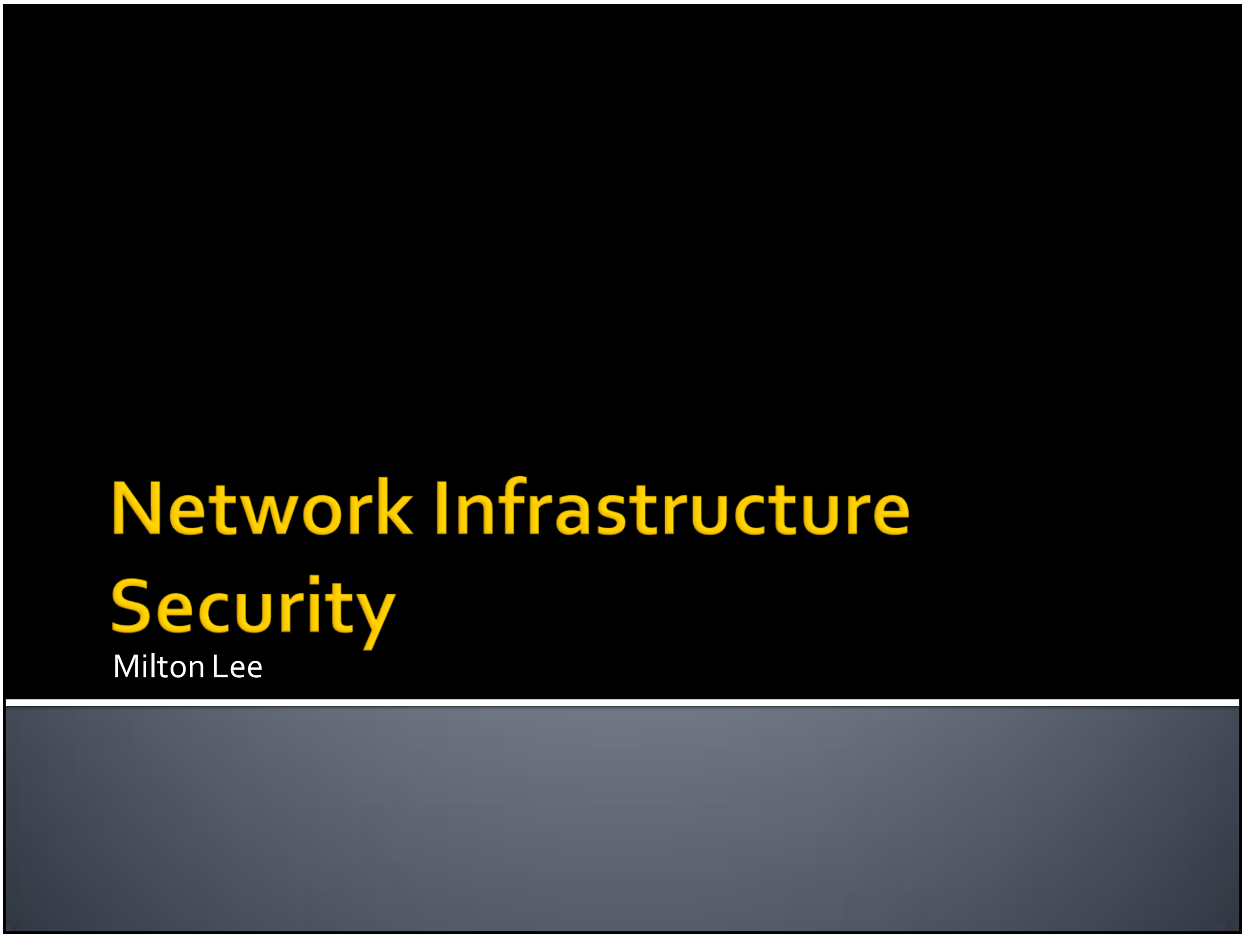
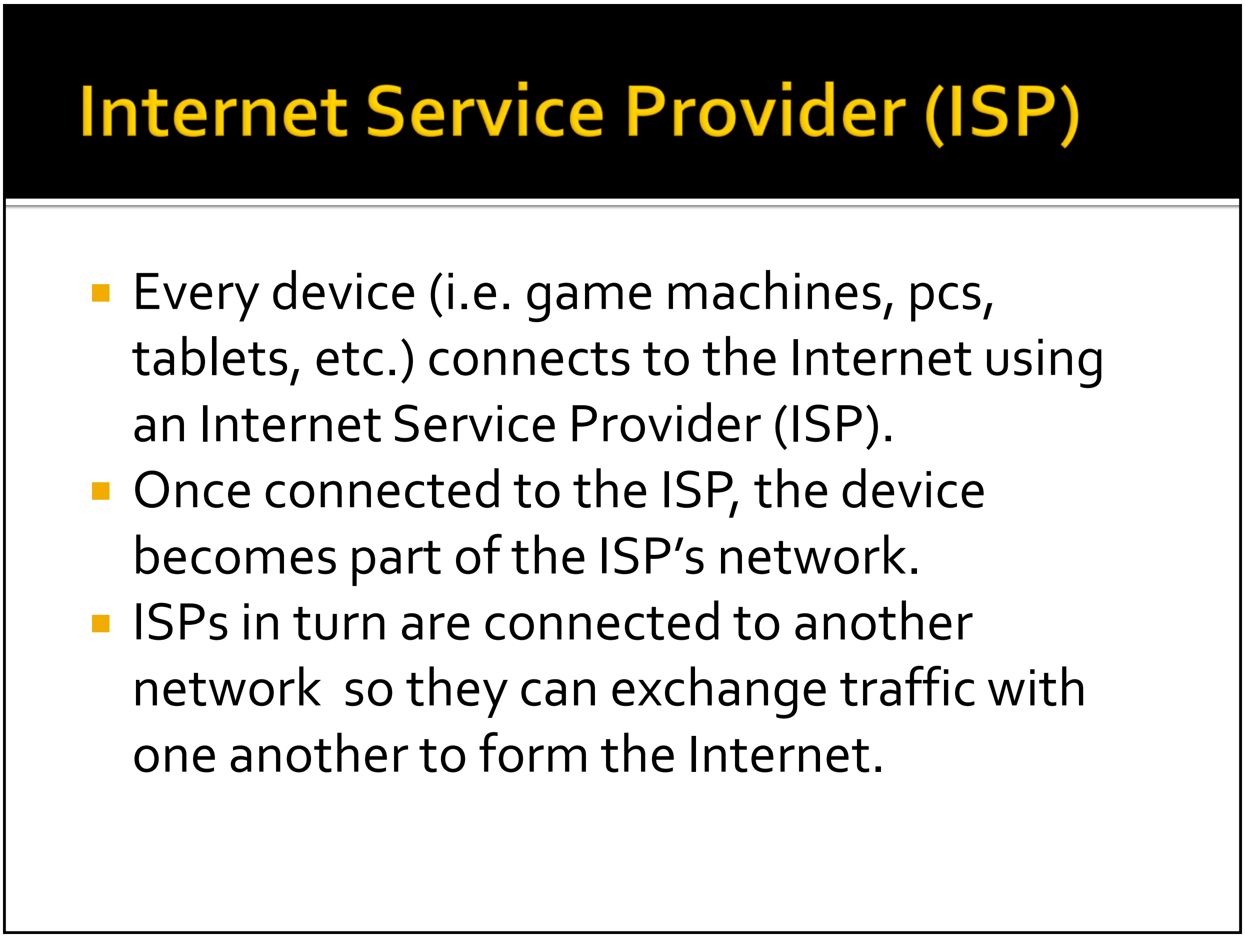


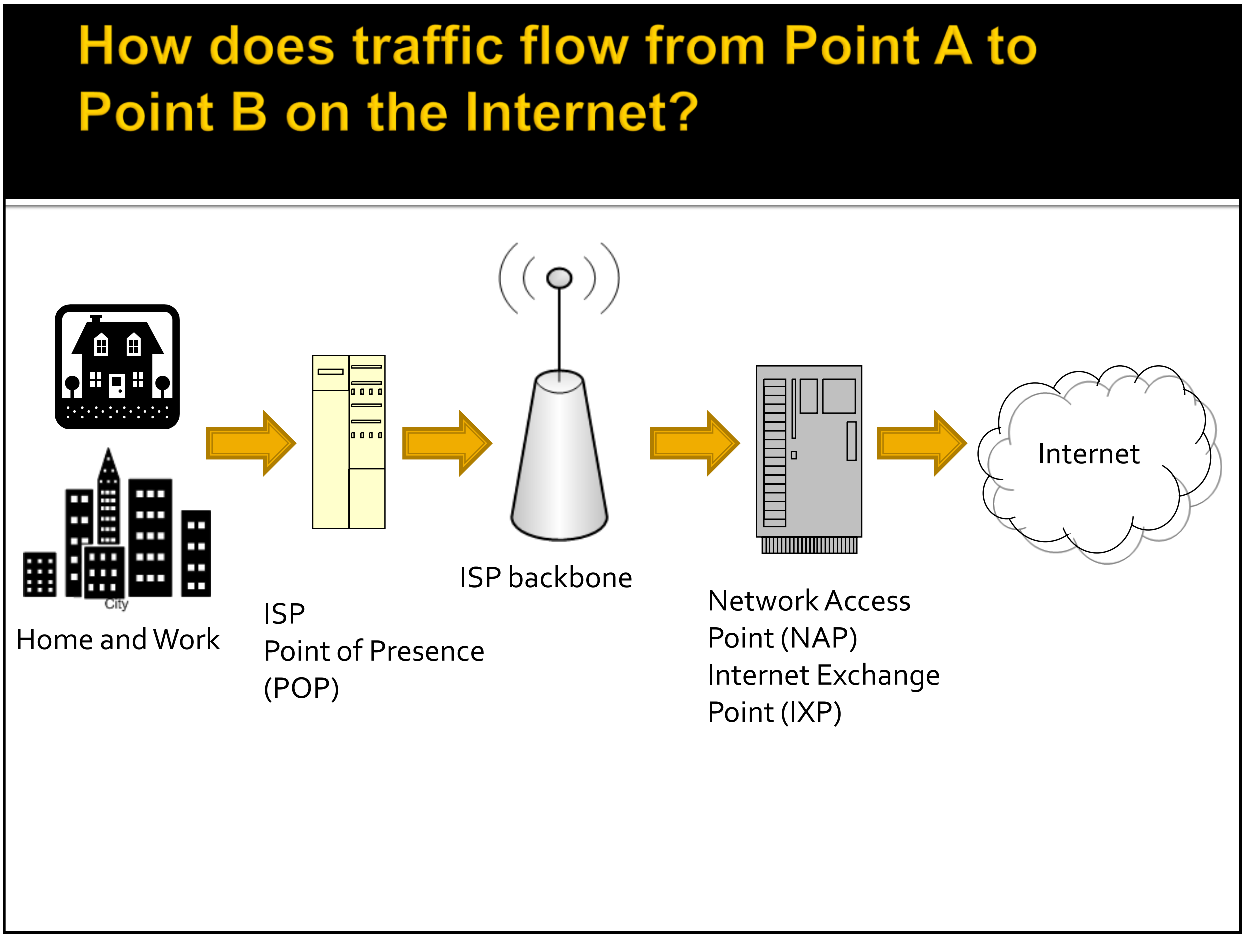
Network Infrastructure Security

Milton Lee



Internet Service Provider (ISP)

- Every device (i.e. game machines, pcs, tablets, etc.) connects to the Internet using an Internet Service Provider (ISP).
- Once connected to the ISP, the device becomes part of the ISP's network.
- ISPs in turn are connected to another network so they can exchange traffic with one another to form the Internet.



How does traffic flow from Point A to Point B on the Internet?

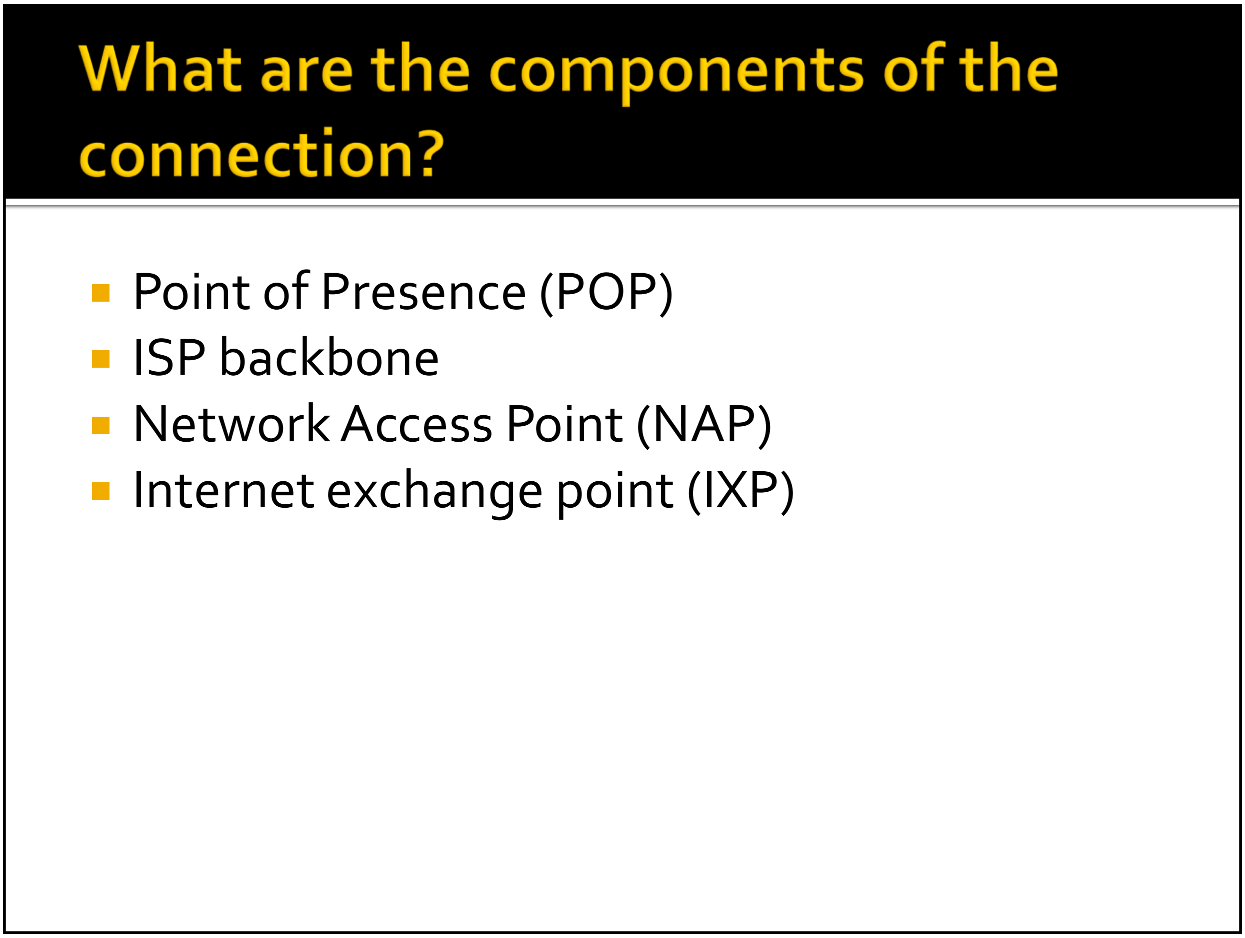
Home and Work

ISP
Point of Presence
(POP)

ISP backbone

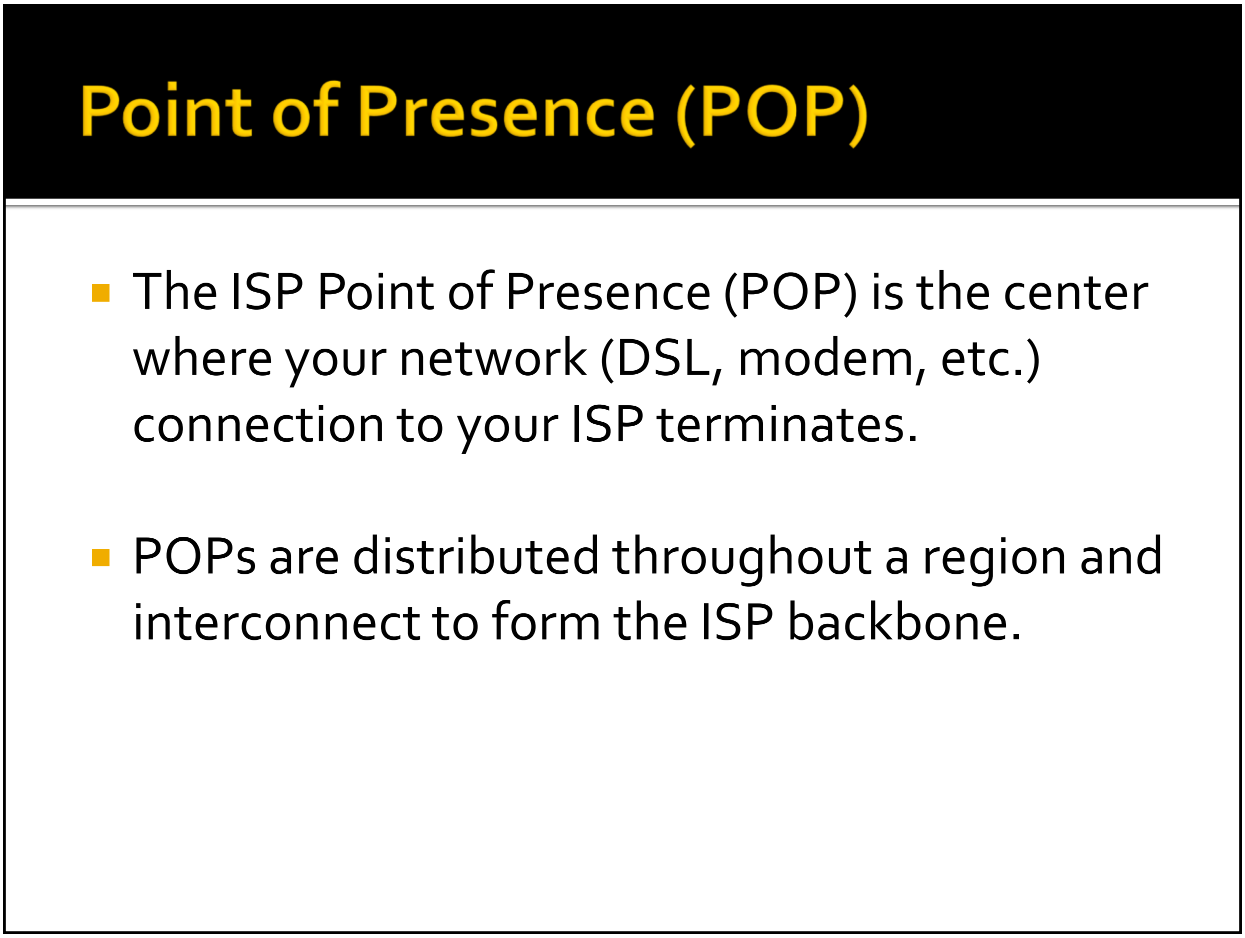
Network Access
Point (NAP)
Internet Exchange
Point (IXP)

Internet



What are the components of the connection?

- Point of Presence (POP)
- ISP backbone
- Network Access Point (NAP)
- Internet exchange point (IXP)

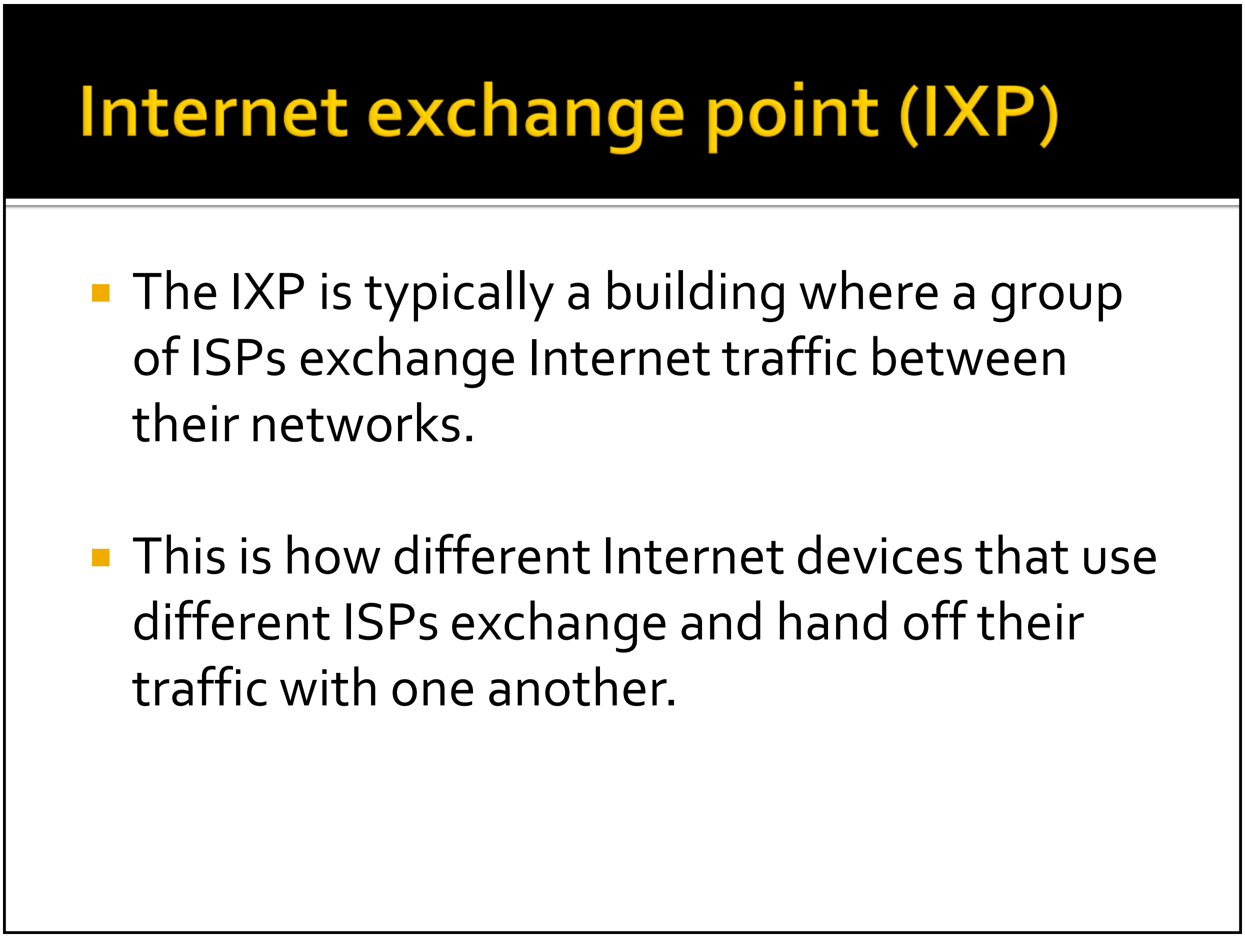


Point of Presence (POP)

- The ISP Point of Presence (POP) is the center where your network (DSL, modem, etc.) connection to your ISP terminates.
- POPs are distributed throughout a region and interconnect to form the ISP backbone.

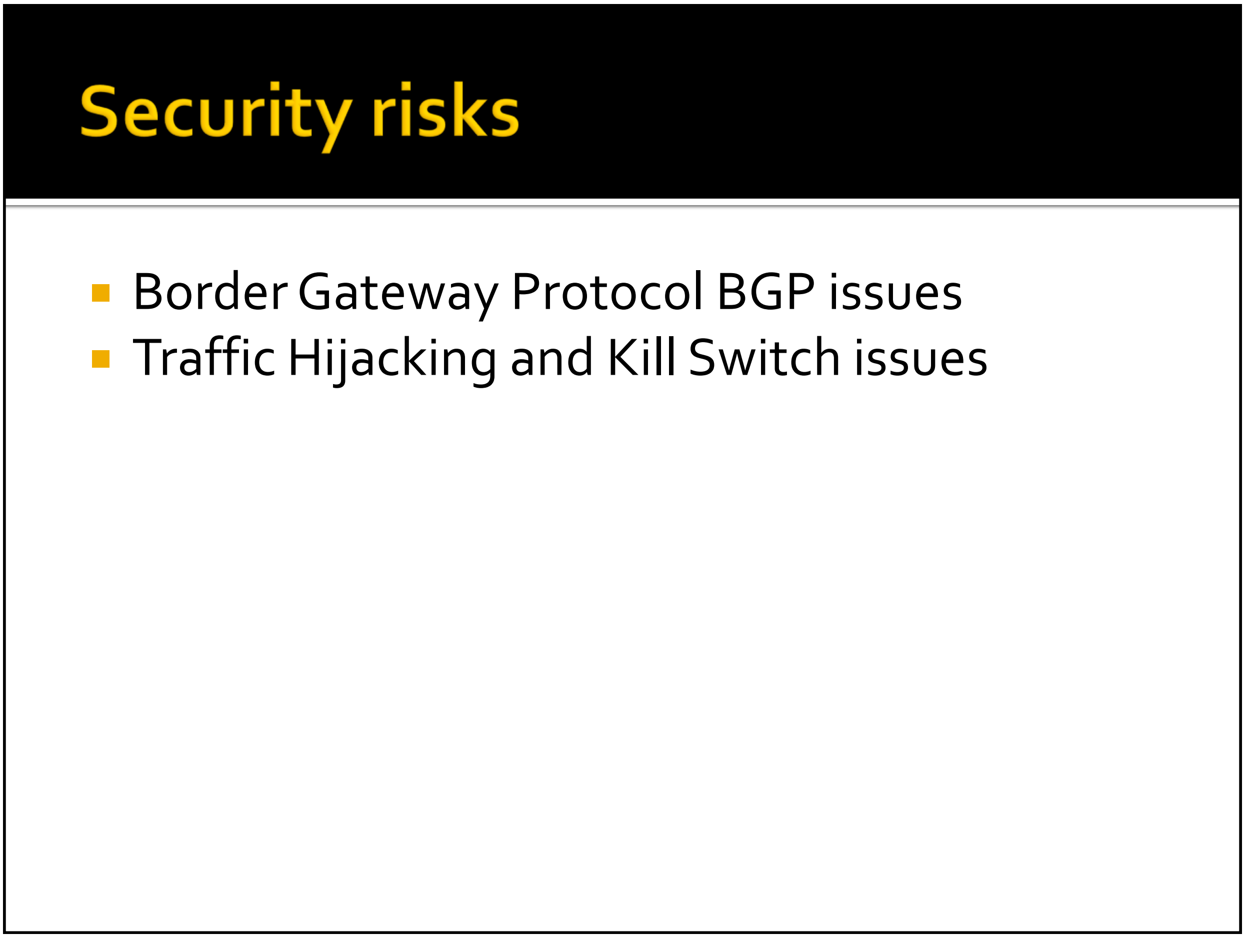
ISP backbone

- The ISP backbone which is comprised of POPs hands off their traffic to Network Access Point s (NAP) or what is now known today as Internet Exchange Points (IXP).



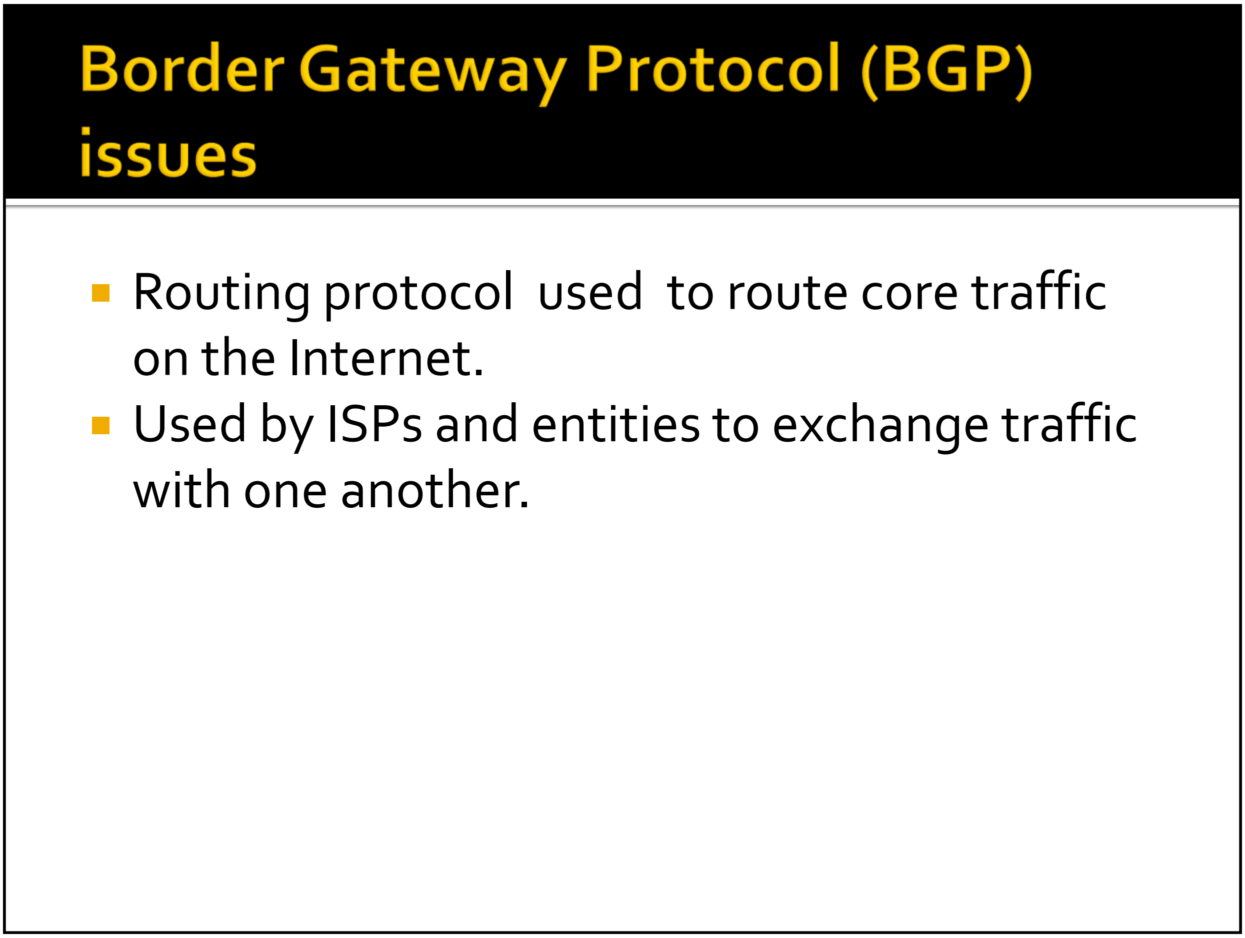
Internet exchange point (IXP)

- The IXP is typically a building where a group of ISPs exchange Internet traffic between their networks.
- This is how different Internet devices that use different ISPs exchange and hand off their traffic with one another.



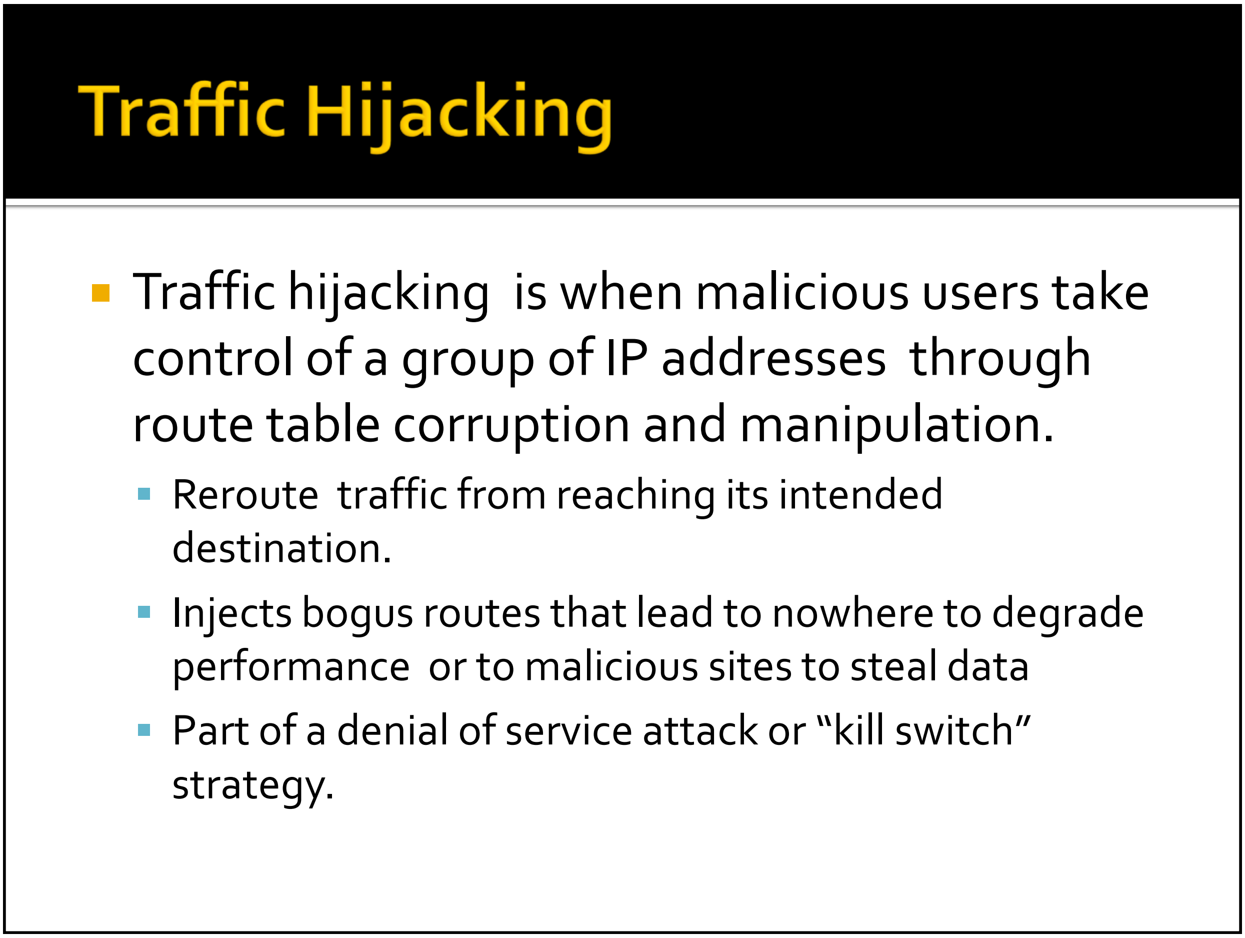
Security risks

- Border Gateway Protocol BGP issues
- Traffic Hijacking and Kill Switch issues



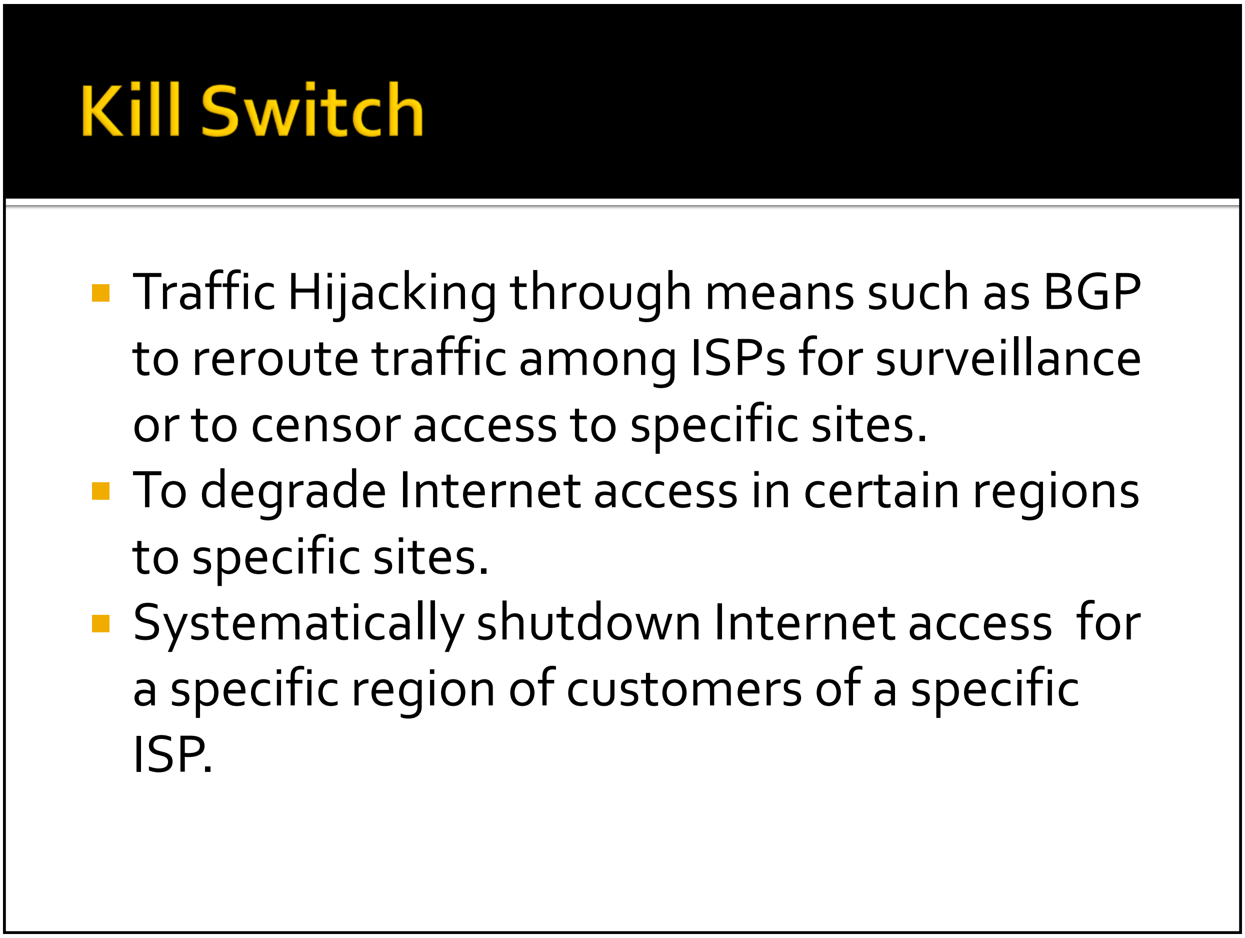
Border Gateway Protocol (BGP) issues

- Routing protocol used to route core traffic on the Internet.
- Used by ISPs and entities to exchange traffic with one another.



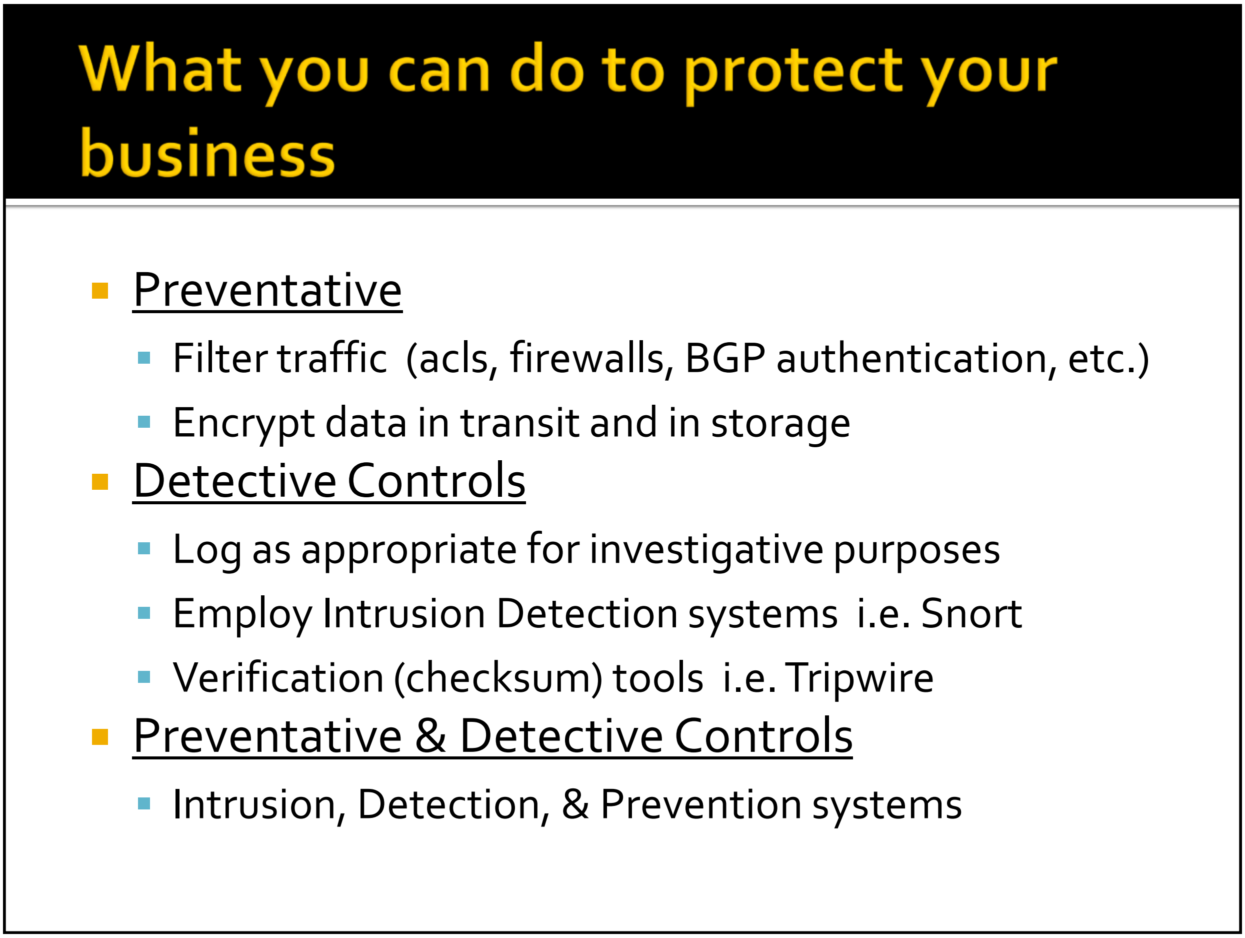
Traffic Hijacking

- Traffic hijacking is when malicious users take control of a group of IP addresses through route table corruption and manipulation.
  - Reroute traffic from reaching its intended destination.
  - Injects bogus routes that lead to nowhere to degrade performance or to malicious sites to steal data
  - Part of a denial of service attack or “kill switch” strategy.



Kill Switch

- Traffic Hijacking through means such as BGP to reroute traffic among ISPs for surveillance or to censor access to specific sites.
- To degrade Internet access in certain regions to specific sites.
- Systematically shutdown Internet access for a specific region of customers of a specific ISP.



What you can do to protect your business

- Preventative
  - Filter traffic (acls, firewalls, BGP authentication, etc.)
  - Encrypt data in transit and in storage
- Detective Controls
  - Log as appropriate for investigative purposes
  - Employ Intrusion Detection systems i.e. Snort
  - Verification (checksum) tools i.e. Tripwire
- Preventative & Detective Controls
  - Intrusion, Detection, & Prevention systems