Security on NKN network

RS MANI

National **Knowledge** Network

THANK YOU

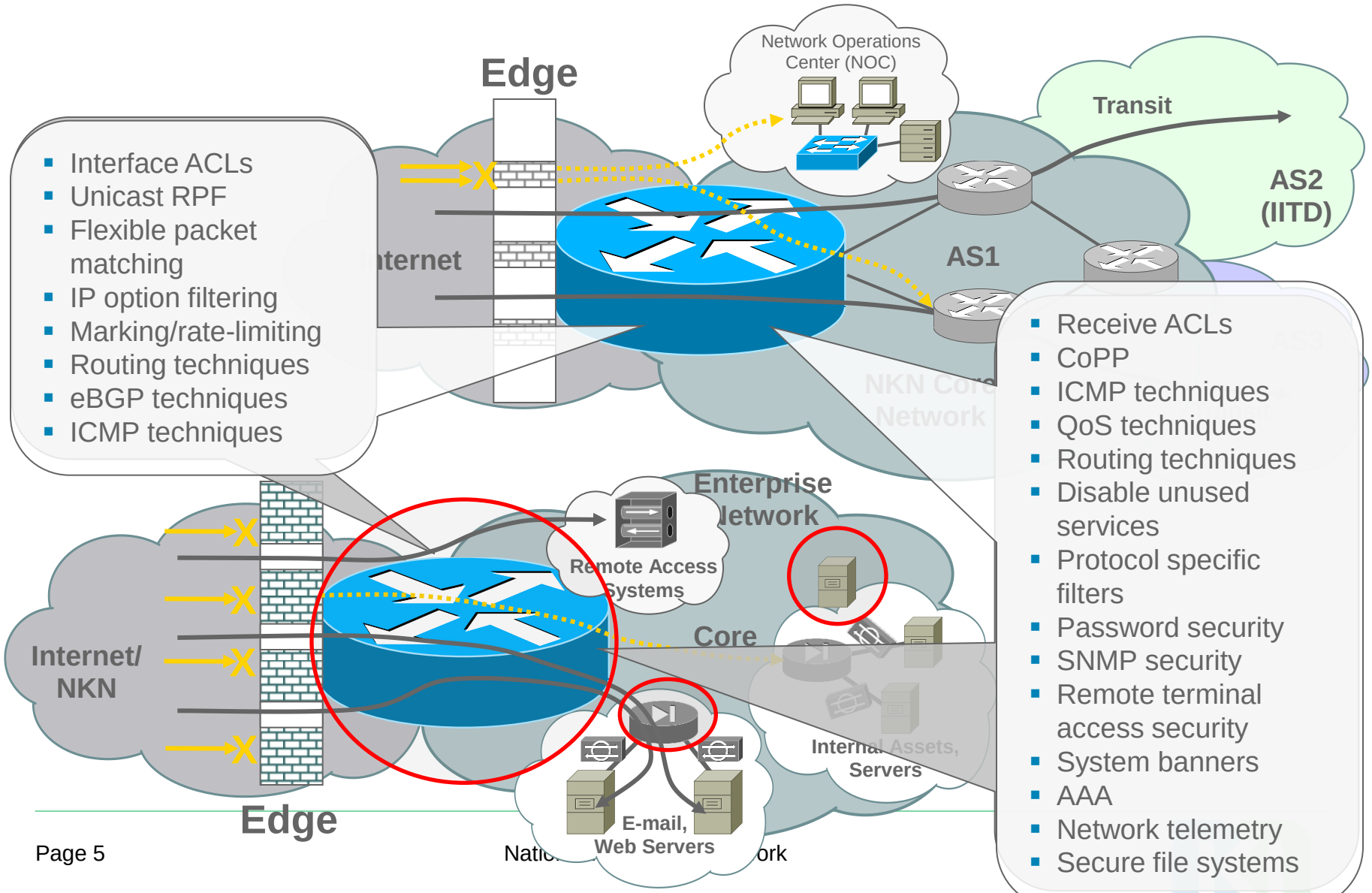
Threat and Attack Categories

Attacks	Description
Resource Exhaustion Attacks	Denial Of Service attack: Either Direct, transit, through reflection.
Spoofing Attacks	Packets that masquerades details like source IP address to gain access which otherwise was denied.
Transport Protocol Attacks	Prevents upper-layer communication between hosts or hijacks established session Exploits previous authentication measures Enables eavesdropping or false data injection
Routing Protocol Attacks	Disrupts routing protocol peering or redirects traffic flows. (Like a device can act as a router and participate with the other legitimate ones)

Threat and Attack Categories(cont.)

Attacks	Description
IP control-plane / IP Services	Attacks against DHCP, DNS, NTP & anything that punts CPU
Unauthorized Access	Attempts to gain unauthorized access to restricted systems and networks. (AAA)
Software Vulnerabilities	Software defect that may compromise confidentiality, integrity, or availability of the device and data plane traffic. (Latest Patches)

Security Applied Up Till Now



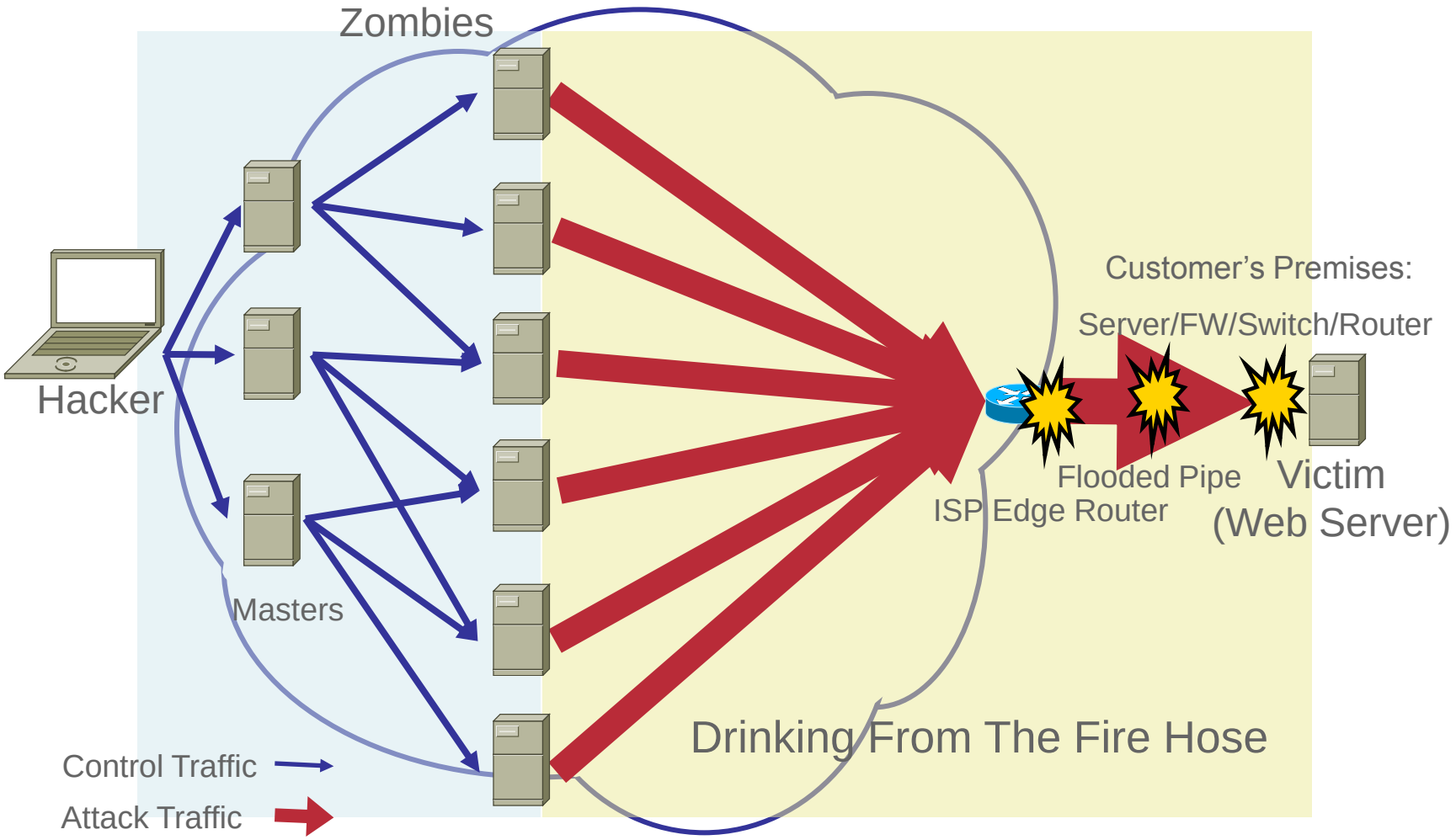
- Interface ACLs
- Unicast RPF
- Flexible packet matching
- IP option filtering
- Marking/rate-limiting
- Routing techniques
- eBGP techniques
- ICMP techniques

- Receive ACLs
- CoPP
- ICMP techniques
- QoS techniques
- Routing techniques
- Disable unused services
- Protocol specific filters
- Password security
- SNMP security
- Remote terminal access security
- System banners
- AAA
- Network telemetry
- Secure file systems

AGENDA

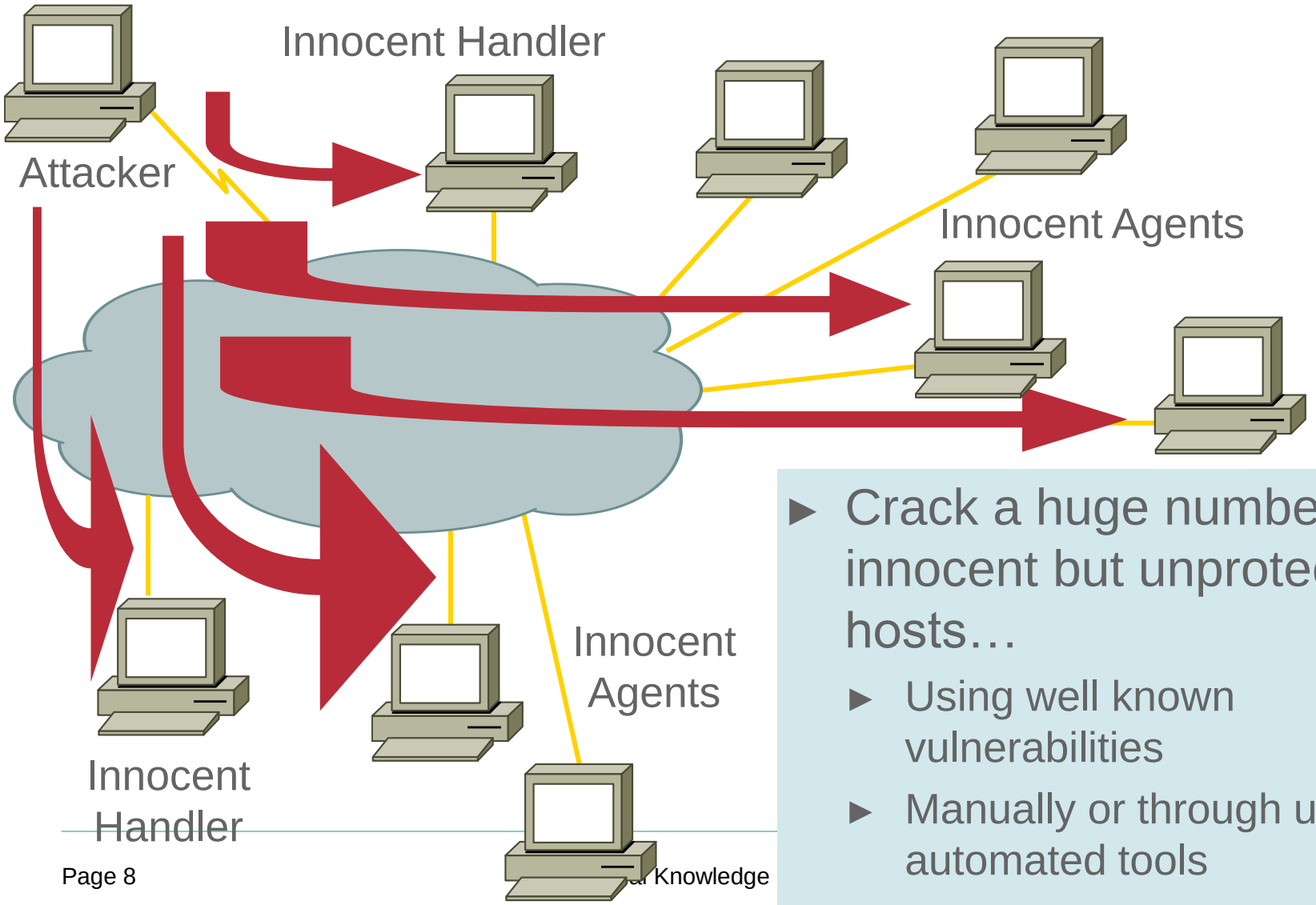
- DDOS—What Is It?
- Examples of DDOS
- Co-lateral Damage
- Origin of BOTNETs
- How BOTNETs are Created
- BOTNET Uses
- BOTNET Mitigation Options

Denial of Service and ISPs



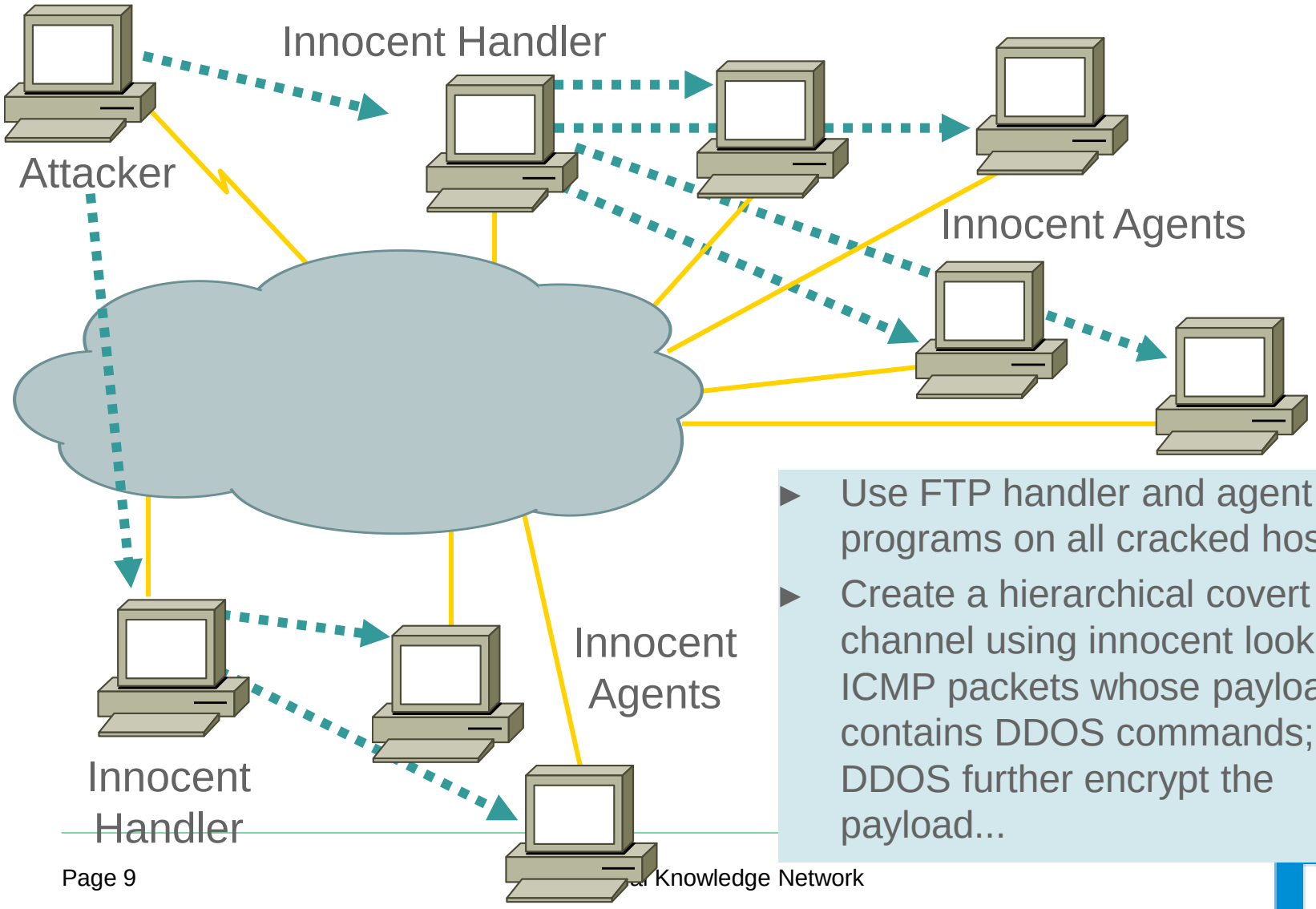
Slide Courtesy of Riverhead networks

DDoS Step 1: Crack Handlers and Agents



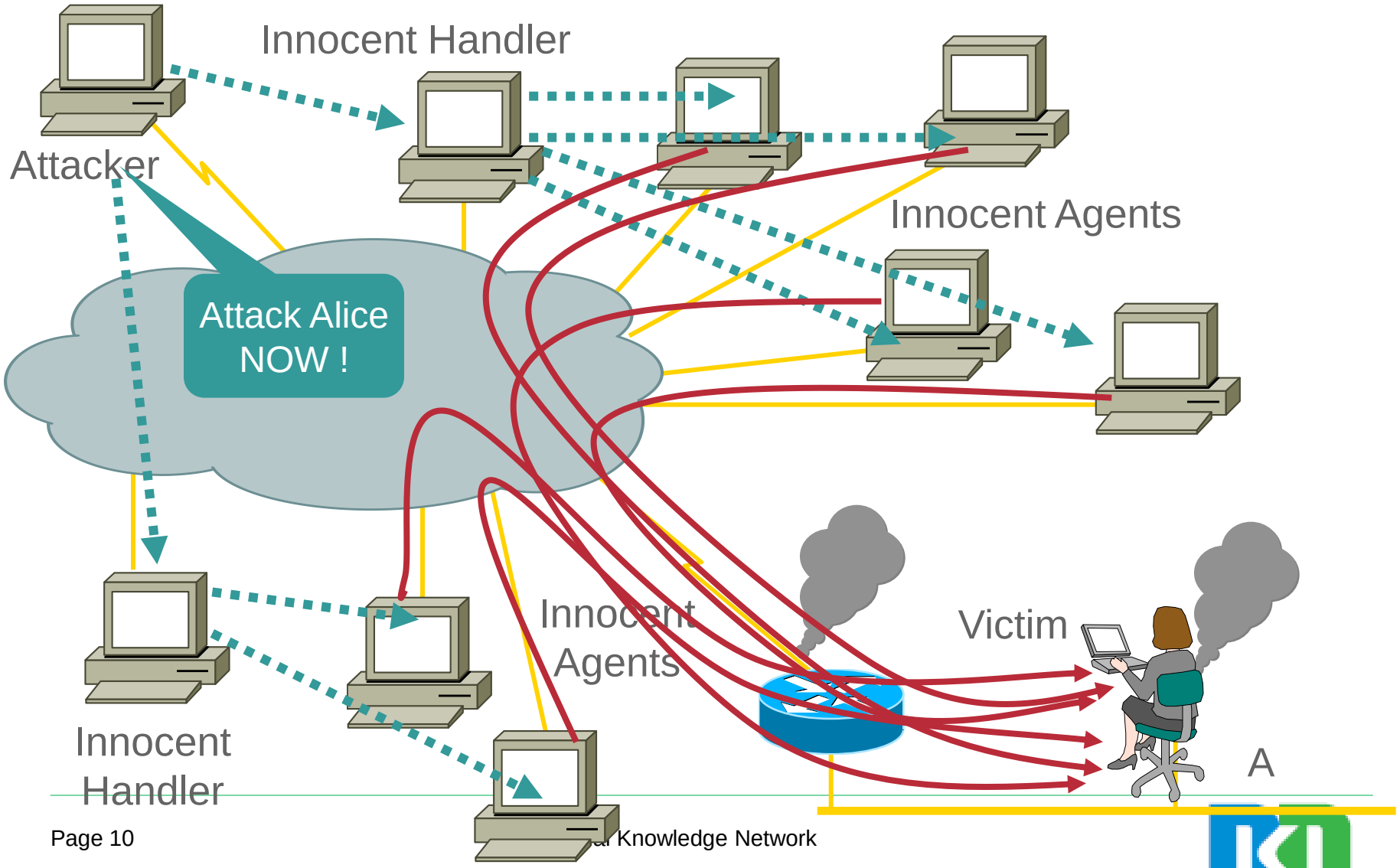
- Crack a huge number of innocent but unprotected hosts…
  - Using well known vulnerabilities
  - Manually or through use of automated tools

DDoS Step 2: Install Trojan & Covert Communication Channel

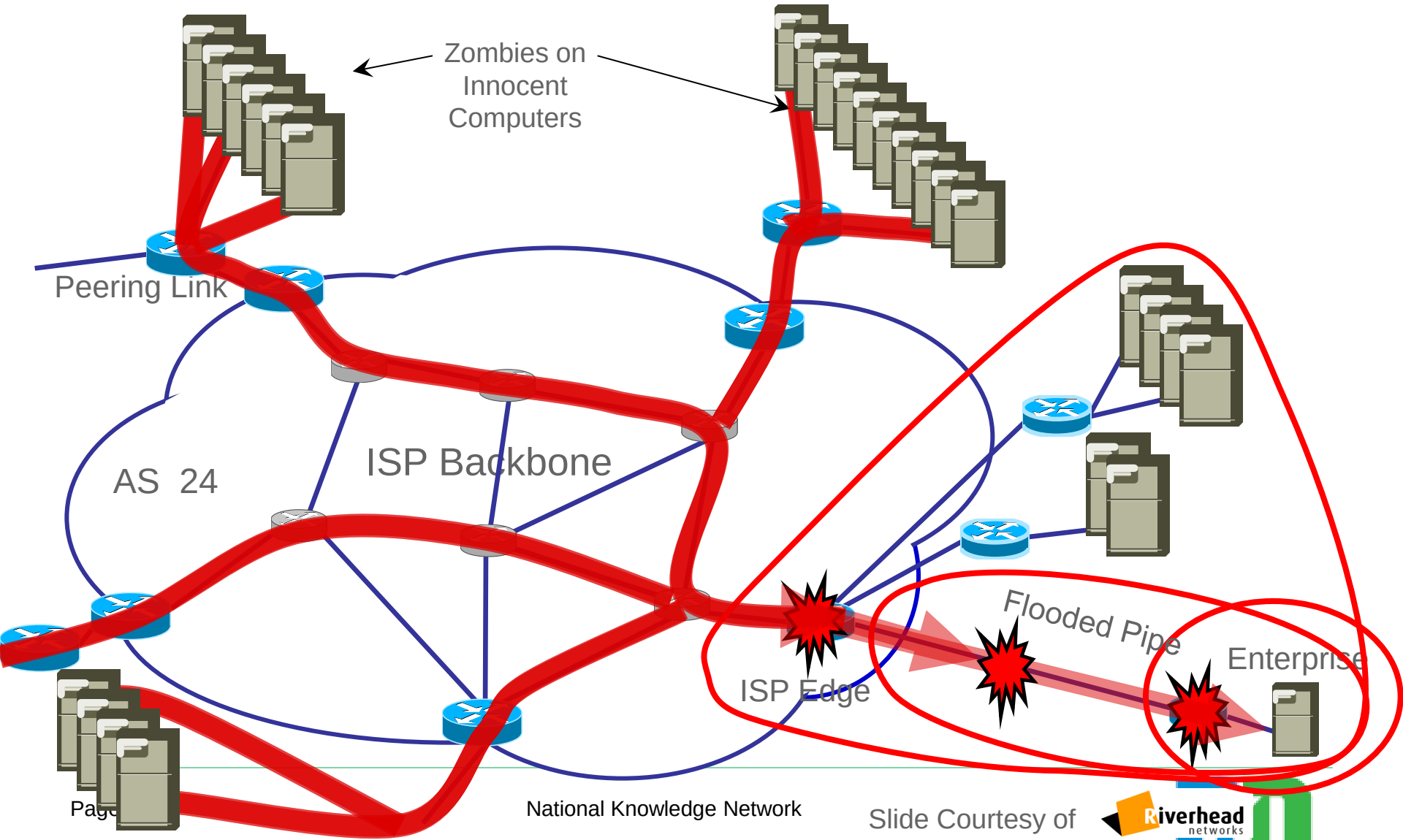


- Use FTP handler and agent programs on all cracked hosts
- Create a hierarchical covert channel using innocent looking ICMP packets whose payload contains DDOS commands; some DDOS further encrypt the payload...

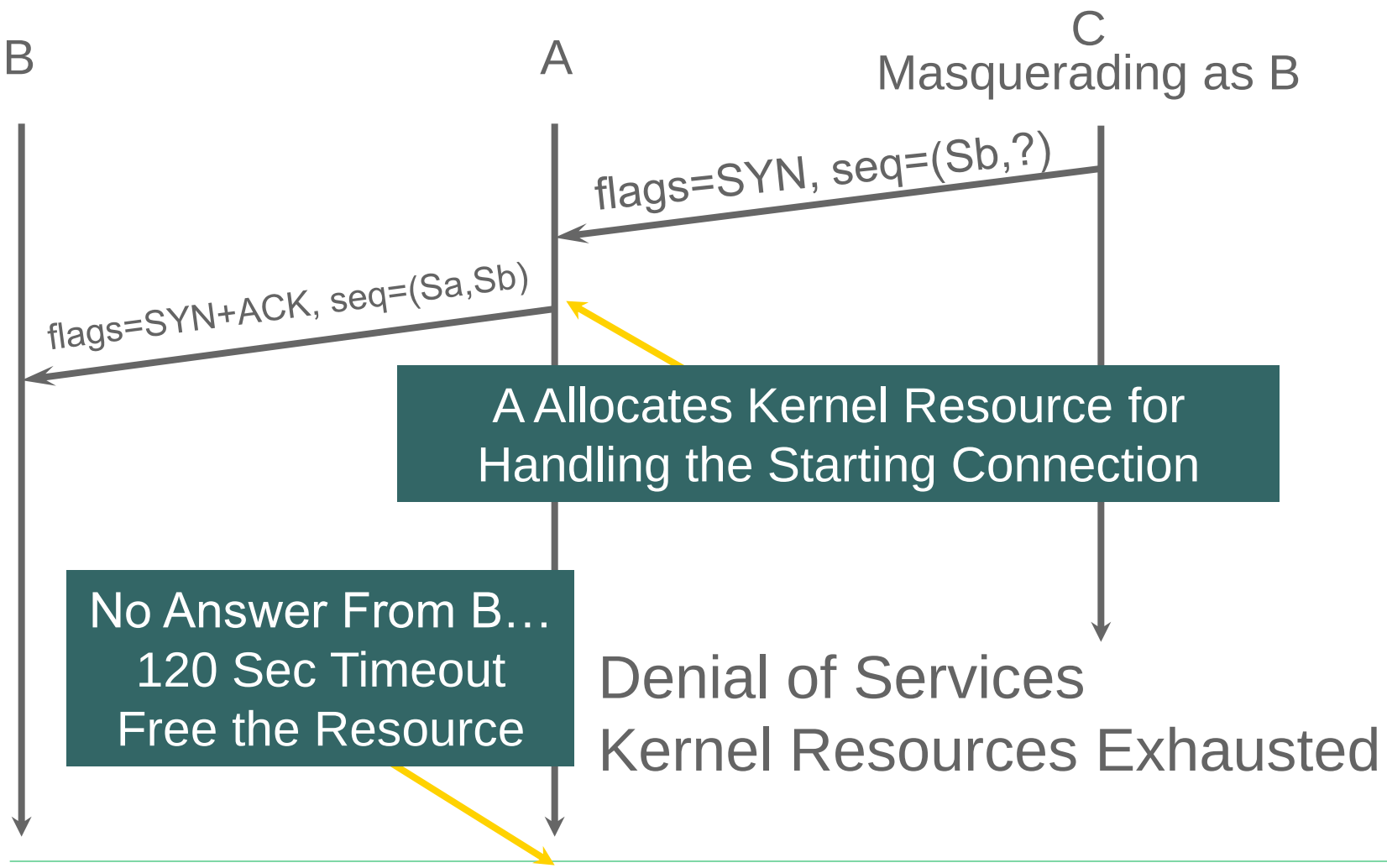
DDoS Step 3: Launch the Attack



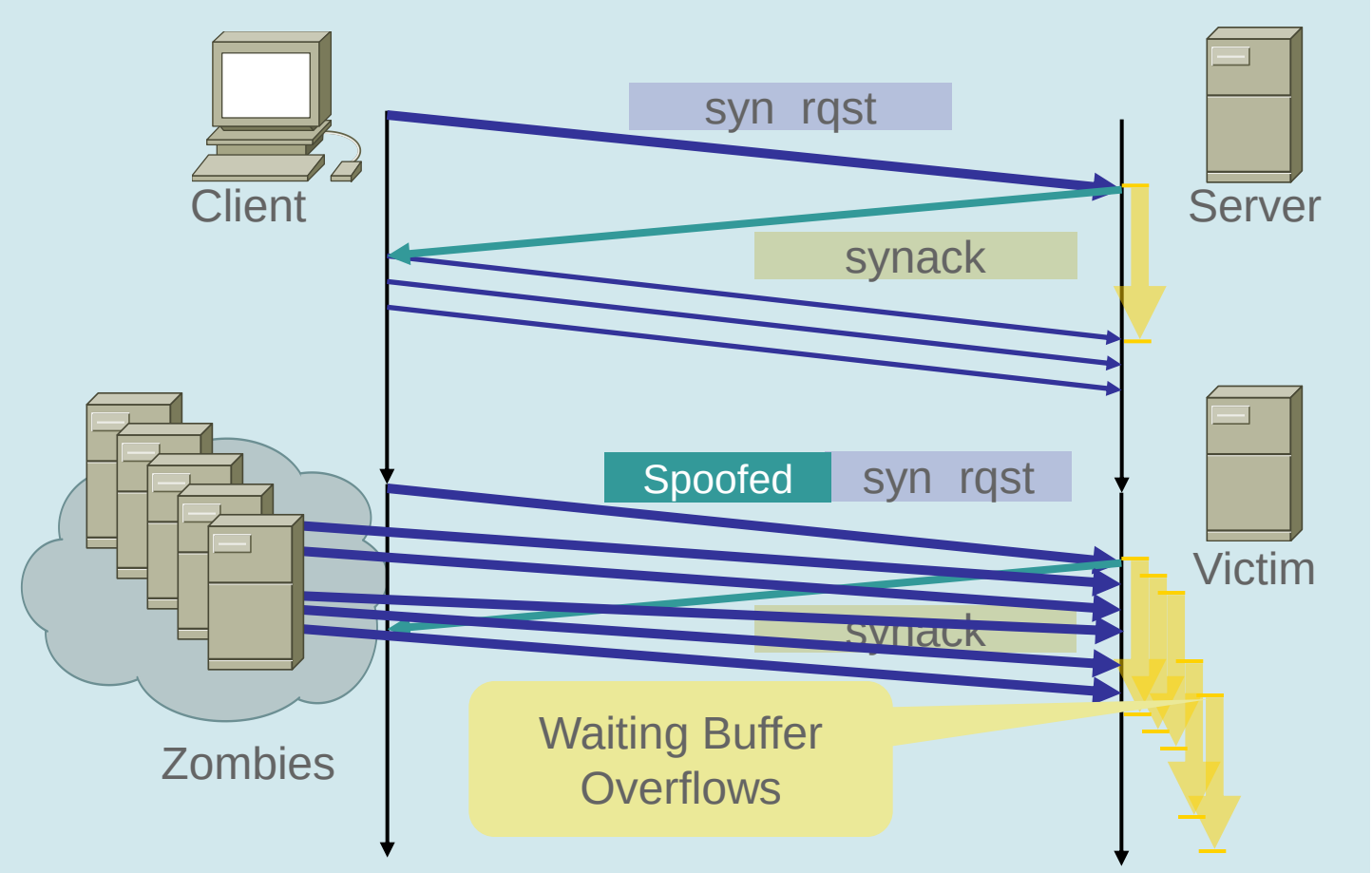
Distributed Denial of Service



SYN Attack


B
A
C
Masquerading as B
flags=SYN, seq=(Sb,?)
flags=SYN+ACK, seq=(Sa,Sb)
A Allocates Kernel Resource for
Handling the Starting Connection
No Answer From B…
120 Sec Timeout
Free the Resource
Denial of Services
Kernel Resources Exhausted

TCP SYN Flood



One of the first CERT DDoS advisories issued – 9/1996

- http://www.cert.org/advisories/CA-1996-21.html

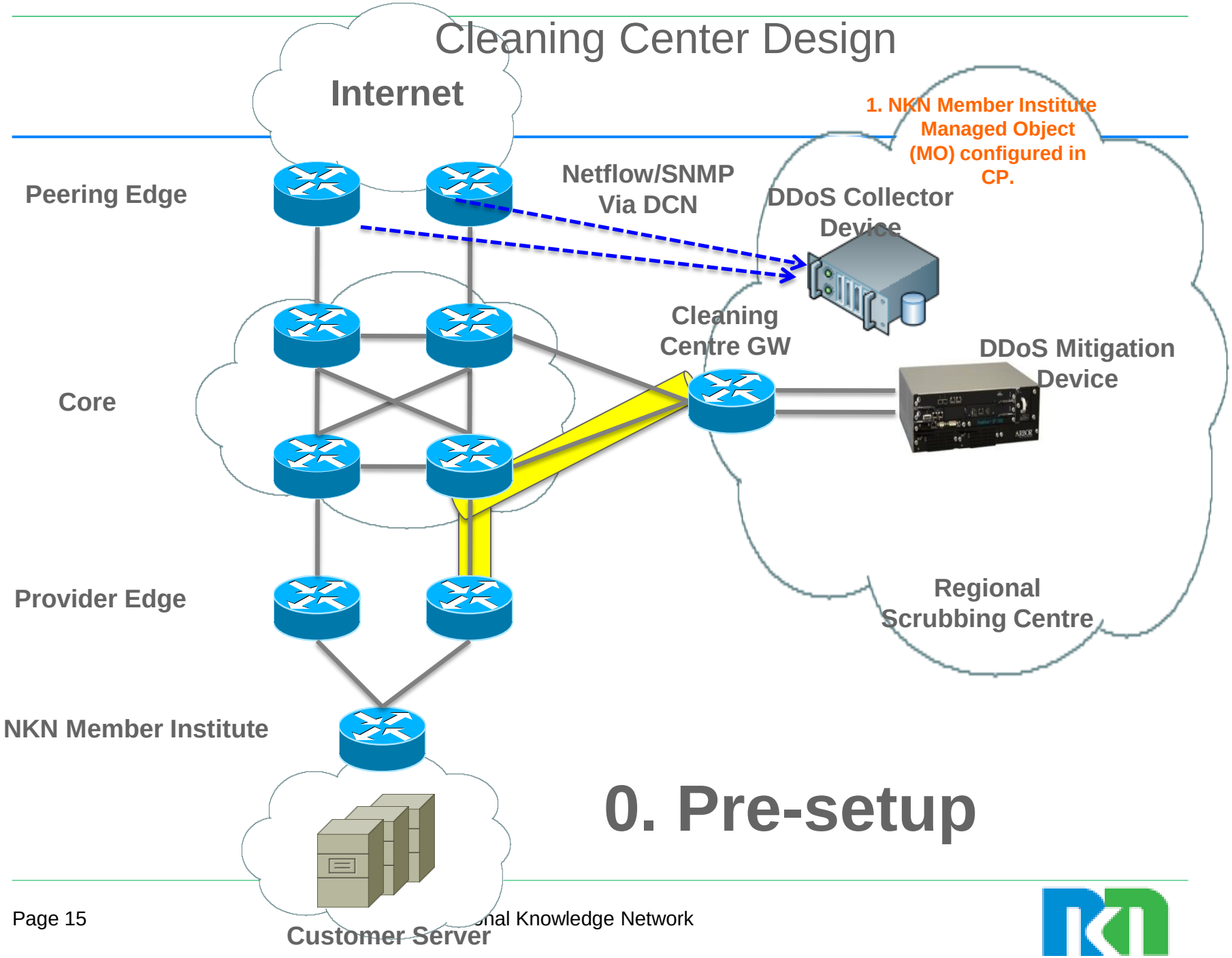
TCP SYN Flood

```
TCP
Local Address          Remote Address         State
-------------------- -------------------- -------
*.*                    *.*                  IDLE
*.sunrpc               *.*                  LISTEN
*.ftp                  *.*                  LISTEN
*.telnet               *.*                  LISTEN
*.finger               *.*                  LISTEN
target.telnet    10.10.10.11.41508          SYN_RCVD
target.telnet    10.10.10.12.41508          SYN_RCVD
target.telnet    10.10.10.13.41508          SYN_RCVD
target.telnet    10.10.10.14.41508          SYN_RCVD
target.telnet    10.10.10.10.41508          SYN_RCVD
target.telnet    10.10.10.15.41508          SYN_RCVD
target.telnet    10.10.10.16.41508          SYN_RCVD
target.telnet    10.10.10.17.41508          SYN_RCVD
target.telnet    10.10.10.18.41508          SYN_RCVD
target.telnet    10.10.10.19.41508          SYN_RCVD
target.telnet    10.10.10.20.41508          SYN_RCVD
*.*                    *.*                  IDLE
```

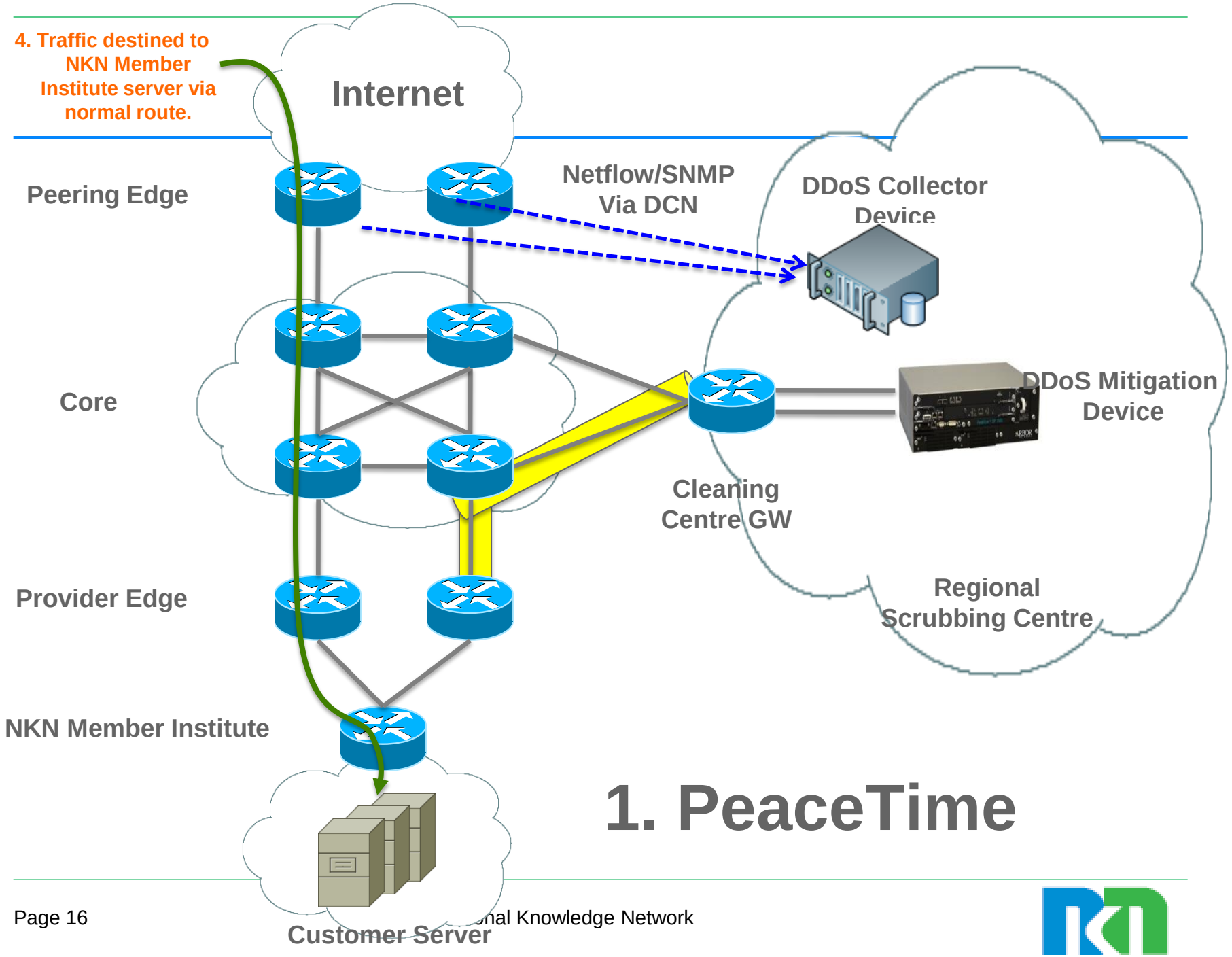
Result of `netstat -a` On Target Host

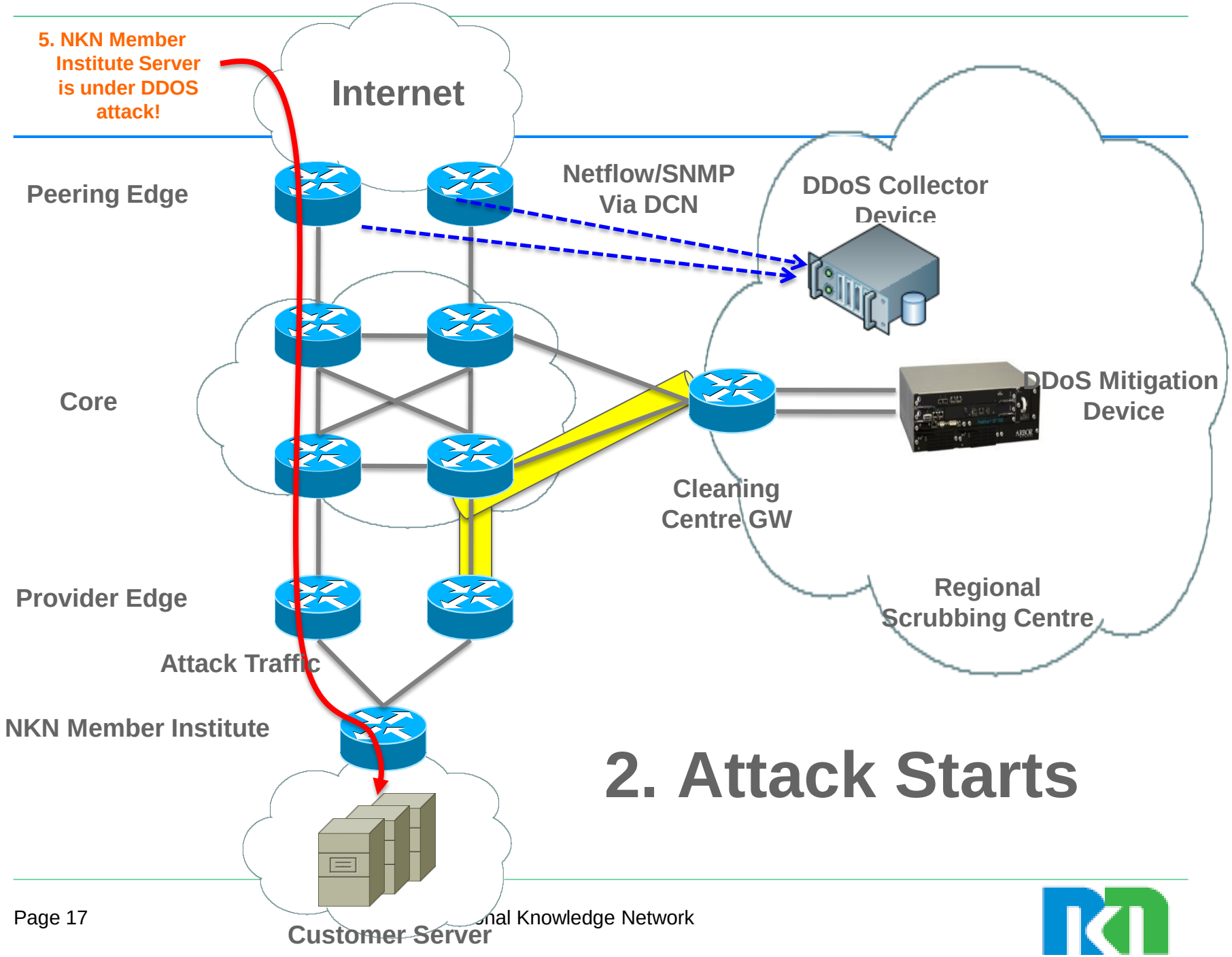
Once the Connection Queue Is Full of Waiting-to-Be-Completed Connections, No More Connections Can Be Accepted on the Target Port

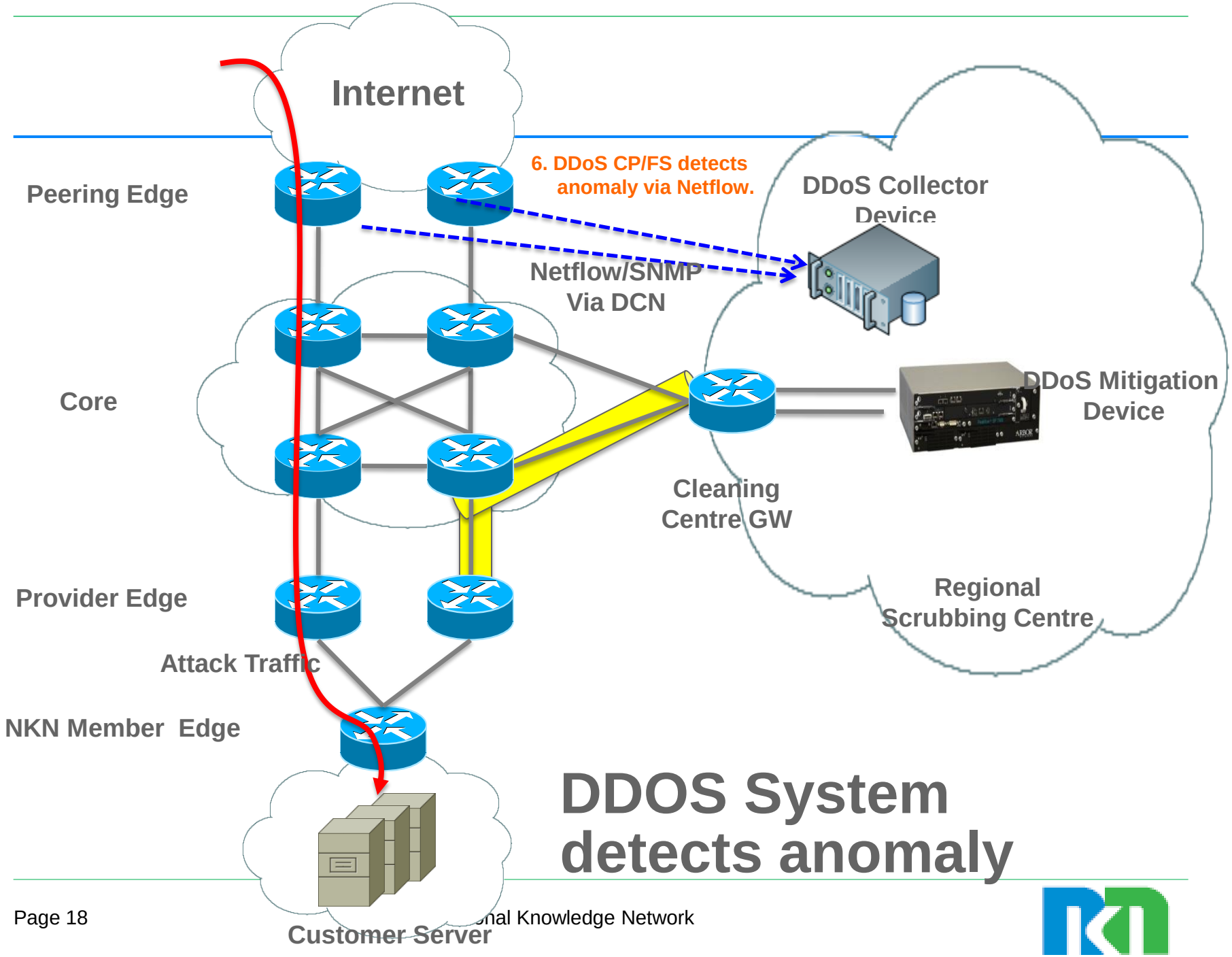
Cleaning Center Design



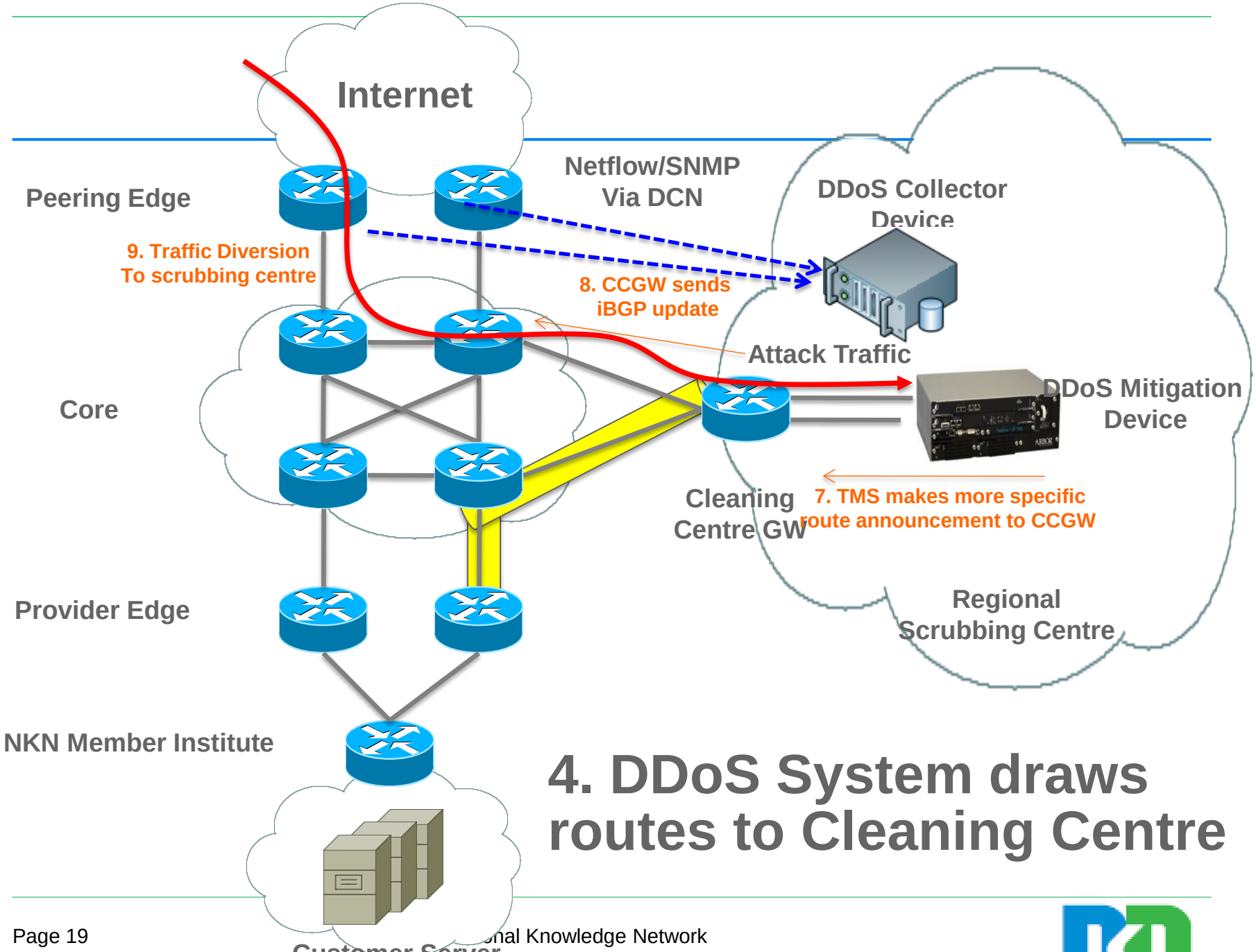
0. Pre-setup


4. Traffic destined to NKN Member Institute server via normal route.
Internet
Peering Edge
Netflow/SNMP Via DCN
DDoS Collector Device
Core
DDoS Mitigation Device
Cleaning Centre GW
Provider Edge
Regional Scrubbing Centre
NKN Member Institute
Customer Server
1. PeaceTime

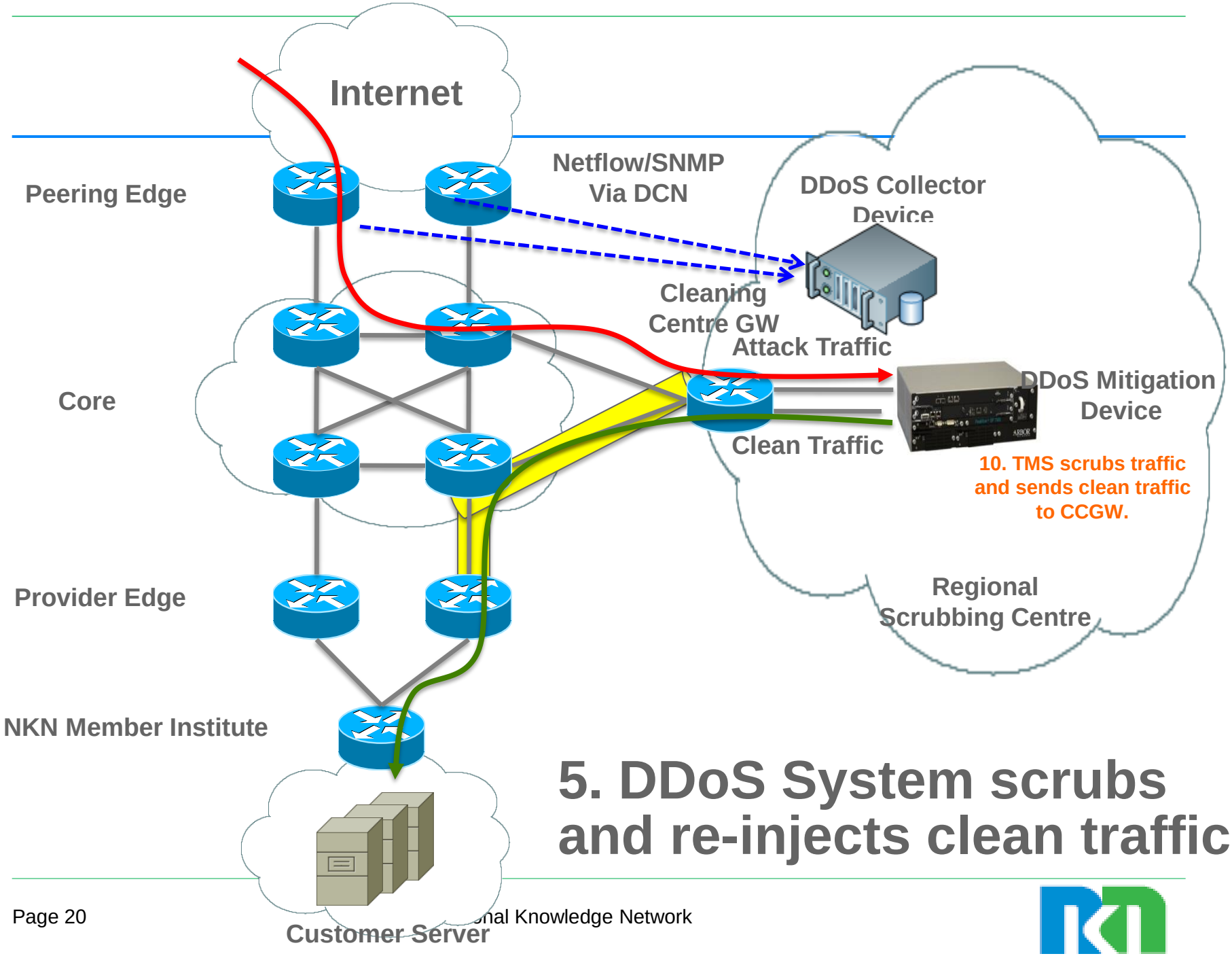

5. NKN Member Institute Server is under DDOS attack!
Internet
Peering Edge
Netflow/SNMP Via DCN
DDoS Collector Device
Core
DDoS Mitigation Device
Cleaning Centre GW
Regional Scrubbing Centre
Provider Edge
Attack Traffic
NKN Member Institute
Customer Server
2. Attack Starts



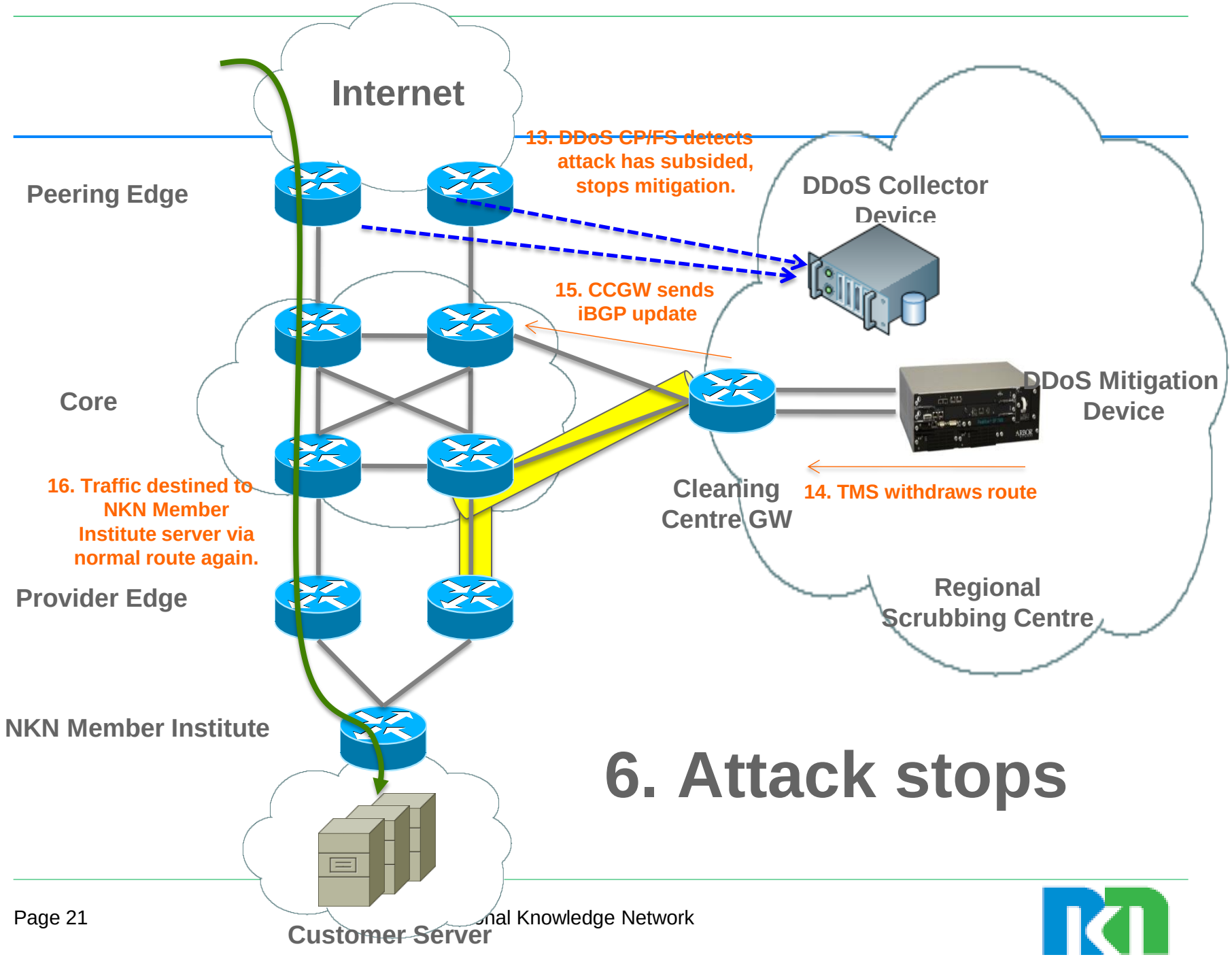
DDOS System detects anomaly



4. DDoS System draws routes to Cleaning Centre



5. DDoS System scrubs and re-injects clean traffic



6. Attack stops

WWW.NKN.IN

Thank You

Project Implementation Unit
National Knowledge Network
iNOC, National Informatics Centre (NIC)
A - Block, C.G.O. Complex, Lodhi Road
New Delhi – 110 003
Website: www.nkn.in
e-mail: piu@nkn.in