Bits, Frames and Packets – Demystifying the Network

Networking 101

for Security Peeps

RVASec 2019

Rick Lull

Agenda

Intro

Why this Talk

What this Talk isn’t

Networking – what, where, why, how

Securing networks

Network Security – what, why, where, how

Closing – Questions and Answers

Introduction – Rick Lull

Rick Lull

- Lead Security Consultant at SyCom Technologies
- Over 20 years in IT Industry
- 15 years in network and network security operations
- Many certifications, past and present

- Small warning: Dad was a sailor; I picked up some of his habits.

Why this talk?

- Networking is a fundamental and foundational service that security practitioners should understand
- Unfortunately, many don’t ☹
- Or they have certain misconceptions or misassumptions about how it works
- Due to that, decisions get made that end up causing friction between the network and security teams
- Defensive security is hard – let’s not make it ANY harder than we have to

What this talk isn’t

- A network architecture or engineering or operations course
- A network security course
- In other words, just listening to me for 50 minutes will NOT make you pass Network+ or CCNA-Security or whatever

Network – What, Why and Where?

- What is a network?
- Why do we have them?
- Where are they?
  - EVERYWHERE!

Networking – How?

- With equipment, of course!
  - Routers, switches, firewalls, bridges, access points, proxies, VPNs, etc
- Before we dive in to all that fun tech stuff, let’s talk about some theoretical models about how we might expect this thought exercise network to work

Networking – How?

- OSI Model
  - A layered model – from the wire to the application

Networking – OSI Model

- Layer 1 – Physical
- Layer 2 – Data Link
- Layer 3 – Network
- Layer 4 – Transport
- Layer 5 – Session
- Layer 6 – Presentation
- Layer 7 – Application

How? OSI Model -> Real World Examples

Layer	Data Unit	Example
Layer 1 – Physical	Bits	Electrical signals on wire, light pulses on fiber, radio waves on wireless
Layer 2 – Data Link	Frames	Ethernet, TDM, Fiberchannel, AppleTalk, TokenRing, ARCNET
Layer 3 – Network	Packets	IP, IPX/SPX
Layer 4 – Transport	Datagram	TCP, UDP, ESP, AH, SAP
Layer 5 – Session	Data	Sockets/Ports
Layer 6 – Presentation	Data	TLS/SSL/MIME
Layer 7 – Application	Data	HTTP

How? OSI Model -> Real World Examples

Layer	Data Unit	Equipment
Layer 1 – Physical	Bits	Cat5, Cat6 and other twisted pair; multimode fiber; single mode fiber; etc
Layer 2 – Data Link	Frames	Switches, bridges, access points, hubs
Layer 3 – Network	Packets	Multilayer switches, routers, firewalls
Layer 4 – Transport	Datagram	Routers, firewalls
Layer 5 – Session	Data	Firewalls, load balancers
Layer 6 – Presentation	Data	Firewalls, load balancers
Layer 7 – Application	Data	PCs, tablets, servers, etc (stuff that talks over the network)

Equipment

Hub: Forwards frames out of every physical connection…

Switch: It learns layer 2 addresses and only sends frames to where they need to go

Router: It learns layer 3 addresses and only send packets to where they need to go

Firewall: It is told to allow only certain layer 4 or 5 traffic (ports and protocols)

Pathing Help

Spanning Tree

Routing protocols

Addressing: Ethernet and IP

Layer 2 : MAC Addresses

MAC address is a 48 bit number, encoded base 16, so it's 0-9 A-F

Represented like 00:00:00:00:00:00 or 0000.0000.0000 or 00-00-00-00-00-00

Layer 3 : IP Address (IPv4)

IP address is a 32 bit number; normally shown as base 10 number

Represented in "Dotted decimal" in the familiar 192.168.1.1

Addressing: Ethernet and IP, continued

Layer 3 : IP Address (IPv6)

IP address is a **128** bit number; eight groups of four hexadecimal digits with the groups being separated by colons

2001:0db8:0000:0042:0000:8a2e:0370:7334

Why do we care about addressing?

- To communicate with other hosts, of course
- Let’s talk about how it talks
- We are going to assume an IPv4 on Ethernet network to make this as simple as possible

Communication

I am 192.168.1.10. I want to talk to 192.168.1.20.

1. I check my network/subnet mask; it's 255.255.255.0, so good news, this is a local address
2. I use ARP to find the MAC address of the IP address that I have, to send frames to, from me
3. I send frames, sourced from my MAC to the MAC of the destination
4. Profit!

Switching

- What just happened was forwarding done at Layer 2.
- This is switching functionality, as we are forwarding based on data link information, across the best path the switch knows about
- Based on our forwarding information base that we build by learning.

Communication

I am 192.168.1.10. I want to talk to 8.8.8.8.

1. I check my network, it's not the same, so this is a remote address.
2. I check my routing table, what route do I use?
3. I need to send my traffic to the gateway for that route
4. I use ARP to find the MAC address of the IP address for the gateway, as it will send these frames on, for me
5. I send frames, sourced from my MAC to the MAC of the gateway
6. The gateway runs through steps 1 – 5 and forwards the traffic on
7. Additional gateways (aka routers) do it until…
8. Profit!

Routing

- What just happened is forwarding done at Layer 3.
- Routing is the process of forwarding traffic across the best path, based on destination network (Usually…)
- Our routing device (a layer 3 object) builds a routing table
- A routing table is a list of the known networks and their paths

Agenda

~~Intro~~

~~Why This Talk~~

~~Networking – what, where, why, how~~

Securing networks

Network Security – what, why, where, how

Closing and QA

Forwarding Safely

- As you can hopefully imagine, security processes exist to help keep this forwarding ability functioning
- At layer 2, we have spanning tree protocol
  - Spanning Tree is an algorithm whose sole reason for being is to build a “loop free topology”
  - Spanning tree sends BPDUs out the configured links, testing to see if they come back.
  - If they come back – there is a loop and it must be stopped!
  - If somebody else’s BPDUs show up, depending on some factors, I might forward, or I might block

Forwarding Safely

- Multiple modes of spanning tree exist
  - Spanning Tree (STP aka basic spanning tree)
  - Rapid Spanning Tree
  - Per-VLAN
  - Rapid Per-VLAN
  - Multiple Spanning Tree (MST)

Forwarding Safely

- BPDU (bridge protocol data unit)
  - Sent out configured ports
  - Used to detect loops and neighbor switches
- Protections:
  - BPDUGuard
    - Disable ports when received
  - Sane configurations and architectures
  - Physical security of equipment, MDF/IDFs

Forwarding Safely

- At layer 3, we have rout**ing** protocols
  - RIP, OSPF, BGP, IS-IS (industry standard)
  - EIGRP (proprietary)

  - Generally, routing protocols are broken down into 3 categories:
    - Distance vector
    - Path vector
    - Link states
  - And two types:
    - Interior gateway protocols
    - Exterior gateway protocols

Forwarding Safely

- Each routing protocol has it's own way that it establishes neighbor relationships and exchange routing information
- Neighbor relationships are often NOT authenticated and/or encrypted
- Some routing protocols broadcast information out
  - Can be easily picked up so it's a great information gathering step for attackers

Forwarding Safely, continued

- Minimize your broadcasts from routing protocols
  - Eliminating them is great, if possible
- Authenticate your routing peers
- Encrypt routing links that traverse non-trusted transit
- Consider BCP38 & 84 and other guidelines to protect against spoofed traffic and invalid reverse paths
- Consider likely attack vectors AND failure scenarios

Forwarding Safely – Hardening the network

- Standard practices apply, of course:
  - Minimize services running on each box
  - Control and audit admin access
    - Via a centralized system, of course
  - You **do** capture syslog, right?
    - Determine what changes/states you alert on
  - Follow the manufacturer's hardening guide, if applicable
    - Sometimes all there is, is a general guideline
  - Patch/upgrade device code
  - For $Deity's sake, don't filter ping internally…

Agenda

~~Intro~~

~~Why This Talk~~

~~Networking – what, where, why, how~~

~~Securing networks~~

Network Security – why, what, where, how

Closing and QA

Network Security - Why

- The network is the underpinning of information systems
- It is a common touchpoint across different users, devices, departments, services, etc
- When you can’t do anything to the endpoint itself, it become a key player in your strategy

- Key building block for defense in depth

Network Security - What

- Categories of network security
  - Visibility and surveillance
  - Network access and segmentation
  - Enforcement

NetSec What -> Real World Examples

Category	Feature Examples	Equipment Examples
Visibility	span sessions, packet capturing, netflow, logging, rogue AP detection,	Network taps/switches, IDS sensors, sniffers, vuln scanners, sandbox, ongoing packet capturing, traffic analytics, honeypots/deception, CASB
Network Access	802.1x, captive portals, SGT, MACSec, posture assessment, segmentation, DHCP snooping,	NAC, RADIUS servers, proxies, VPN
Enforcement	ACLs, fail closed, posture, segmentation,	Firewalls, proxies, IPS, sandbox, DLP, web filtering, blacklists, whitelists

Network Security - What

- By the way..
  - Consider how all this stuff integrates (or doesn't)
  - How it updates/upgrades
  - How hard it is to get solid results out of it (aka ROI)

Network Security – Where in General

- Deployment of controls should be driven by your security architecture
- Your architecture should be based on your level of risk
- Where are your assets?
  - Is the computer/server/phone the asset or is it your data?

Network Security – Where

- Internet Edge
- Internetwork edge (extranets, vendor connectivity, VPNs)
  - Maybe your WAN edge too
- Data Center
  - East-West traffic between VMs is hard to see and can be $$$ to get, if you aren't very granular
    - Containers probably make this worse
- Cloud
  - IaaS & PaaS; not as much when we are talking SaaS [probably]
- Don't forget about all that encrypted traffic

Network Security – How

- Take stock of what you have
- Close the gap(s) that give you the biggest bang for the buck now, even with an imperfect solution
  - Iterate, iterate, iterate
- Engage the network team
  - Make them the Ally, not the enemy.

Agenda

~~Intro~~

~~Why This Talk~~

~~Networking – what, where, why, how~~

~~Securing networks~~

~~Network Security – why, what, where, how~~

Closing and QA

Suggested References

Cisco CCNA Courses

Wikipedia entries for OSI, IP and other protocols

TCP/IP Illustrated, Volume 2 or whatever they are up to now

ArsTechnica's networking FAQ:
https://arstechnica.com/civis/viewtopic.php?f=10&t=49810

Questions?

Your Questions and Comments?

Contact

Rick Lull

rlull@sycomtech.com

https://www.linkedin.com/in/rick-lull-3aa03666