ALGONQUIN COLLEGE

WEEK 12: SECURITY AND TROUBLESHOOTING

Marvin Krym

April 6, 2016

Troubleshooting Commands

- ipconfig
- arp
- ping
- traceroute
- netstat
- nslookup
- Wireshark
- Carrier light

ipconfig

- Purpose:
  - Windows utility to obtain IP usage information

- Options and Usage:
  - ipconfig: obtain basic IP configuration information: host IP address, mask, gateway, MAC address
  - ipconfig /all includes additional IP information: DNS, DHCP server addresses
  - ipconfig /flushdns
  - ipconfig /release and ipconfig /renew: get updated IP information

arp

- Purpose:
  - utility to manage the arp cache.
- Options:
  - arp –a: show the arp cache
  - arp –d * : delete the contents of the arp cache
- Uses:
  - discover the MAC address of devices in the same network segment

ping

- Purpose:
  - utility to send echo request message and obtain response from any layer 3 connected device. Uses ICMP protocol. (Internet Control Messaging Protocol)

- Options:
  - ping ipaddr: send an echo request to ipaddr
  - Ping ipaddr **-t**: continuously send a ping to ipaddr

- Uses:
  - Verify a layer 3 path to an end device such as a gateway router
  - Simple assessment of packet delay and packet loss

tracert

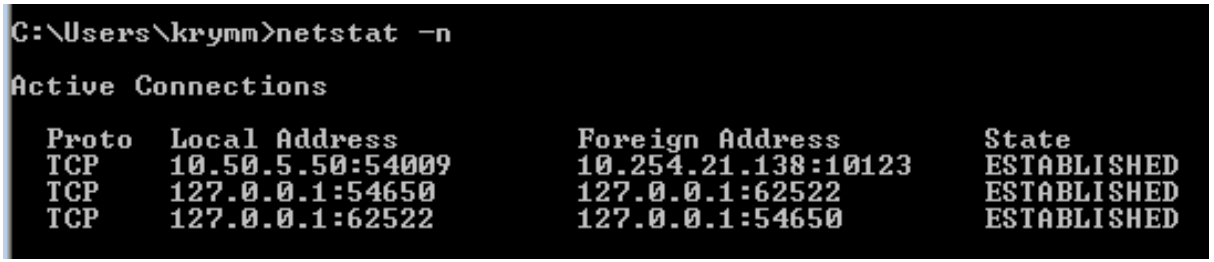
- Purpose:
  - utility to identify the layer 3 path to a destination device.
  - Uses ICMP Protocol

- Options:
  - tracert ipaddr: show the layer 3 path to ipaddr

- Uses:
  - show the layer 3 path
  - identify elements of the routing table
  - identify number of routers in the path to the destination

netstat

- Purpose:
  - utility to display TCP connections including source and destination sockets.



- Options:
  - netstat: show TCP connections
  - netstat –n: show the TCP connections using numeric addresses

nslookup

- Purpose:
  - utility to query the DNS server.
- Options:
  - nslookup URL: translate the URL into an IP address
- Uses:
  - verify DNS configuration
  - get IP information
  - verify connectivity to DNS server

route print

- Purpose:
  - Windows Utility to show node routing table
- Options:
  - route print

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      10.50.5.1      10.50.5.50     10
         10.50.5.0    255.255.255.0         On-link      10.50.5.50    266
        10.50.5.50  255.255.255.255         On-link      10.50.5.50    266
       10.50.5.255  255.255.255.255         On-link      10.50.5.50    266
         127.0.0.0        255.0.0.0         On-link       127.0.0.1    306
         127.0.0.1  255.255.255.255         On-link       127.0.0.1    306
   127.255.255.255  255.255.255.255         On-link       127.0.0.1    306
         224.0.0.0        240.0.0.0         On-link       127.0.0.1    306
         224.0.0.0        240.0.0.0         On-link      10.50.5.50    266
   255.255.255.255  255.255.255.255         On-link       127.0.0.1    306
   255.255.255.255  255.255.255.255         On-link      10.50.5.50    266
===========================================================================
Persistent Routes:
  None
```

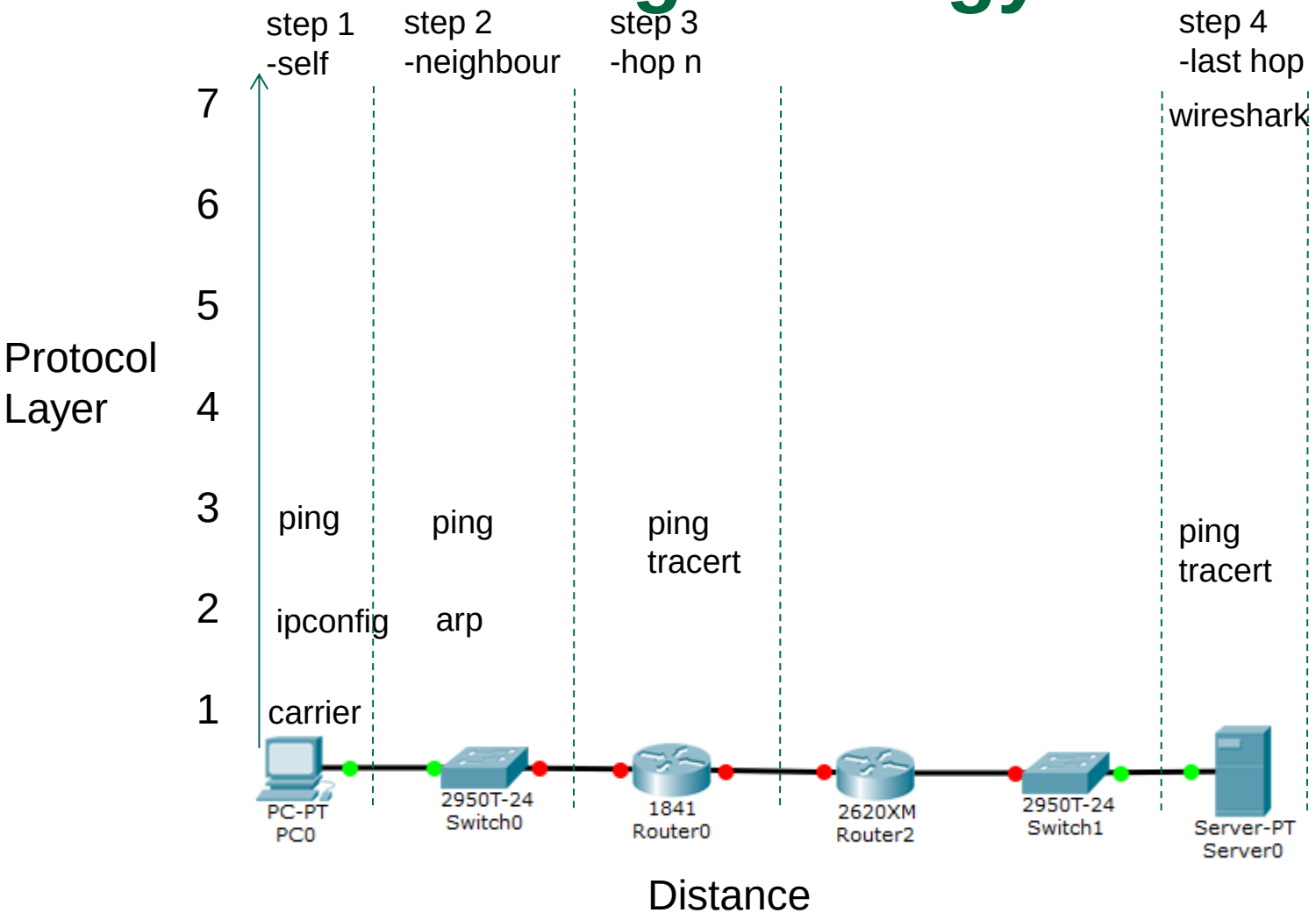
Carrier indicator

- Purpose:
  - Verify physical connection.

- Options:
  - Observer carrier indication on Ethernet port

- Uses:
  - Verify cable connection and integrity
  - Verify NIC

Troubleshooting Strategy



Network Design

- Data Network
- Management
  - Observable
  - Controllable
- Security
- Resiliency
  - Survive Single Points of Failure
- Performance and Capacity
  - Delay
  - Traffic Volume (Packets per Second)

Network Operations

- Monitoring and Control
- Troubleshoot and Repair
  - Failure
  - Performance
- Forecasts and Upgrades
  - Features
  - Growth
  - Technology
- Backup and Restore

Elements of Security

- Data Privacy
  - Data Encryption
- Access Security
  - Device/Network Vulnerabilities
  - Weak Passwords
  - User Authentication and Authorization
  - Physical Security
- Data Integrity
  - Altered Data
  - Redundancy Check Words
  - Digital Hash
- Non Repudiation
  - Digital Signatures
- Denial of Service
  - Wireless Jamming
  - DoS Attacks