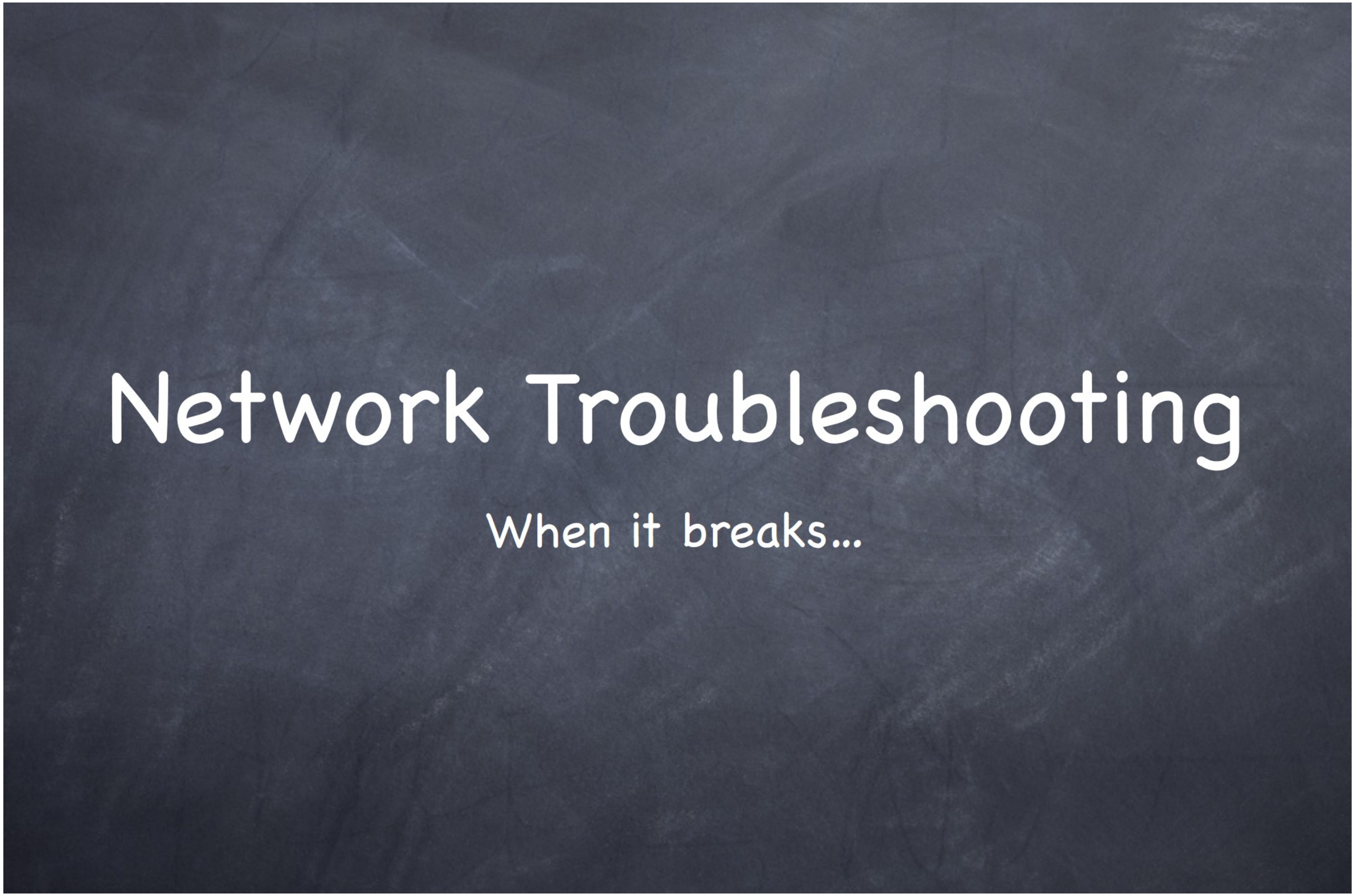
IT 609
Network and System Administration

Network Trouble Shooting

Thursday November 04, 2021

Network Trouble Shooting



Network Troubleshooting

When it breaks...

Command - ping

ICMP - Internet Control Message Protocol

Tests - IP communications (and all lower levels)

Send message out and back

Tracks responses and response time

- Round-trip latency

Unfortunately often blocked by many systems as it can be a probing tool

Command - traceroute

tracert on Windows

Tests - IP communications (and all lower levels)

Ping on steroids

Every router is requested to respond back

Map the pathway through the network

Useful for finding routing issues

Command - nslookup/dig

Tests - DNS function and information

Query to the local DNS server

Simplest use is to do name to IP and IP to name resolution

With additional arguments, can also query specific kinds of records (MX, SOA, SRV, NS, etc)

Command - telnet

Tests - TCP communication (and all lower levels)

Telnet is a remote shell protocol that normally runs on TCP 23

Can also use telnet to open a TCP connection to any port to see if the port is open - listening and accepting connections

Means that the application you are trying to reach is running and open for business

Unfortunately telnet has been deprecated in favor of SSH and often is no longer available

Command - netcat

Tests - TCP communication (and all lower levels)

netcat - replacement for telnet for testing purposes

“nc” on Unix

Can also do UDP

Command - netstat

Tests - current state of network connections on a computer

Shows currently open connections (incoming and outgoing) as well as open ports that are listening

Command - tcpdump

Tests - capture/dump network traffic for analysis

Not as richly featured as Wireshark, but built into most Unix systems and easily available

Windows has “netsh trace”