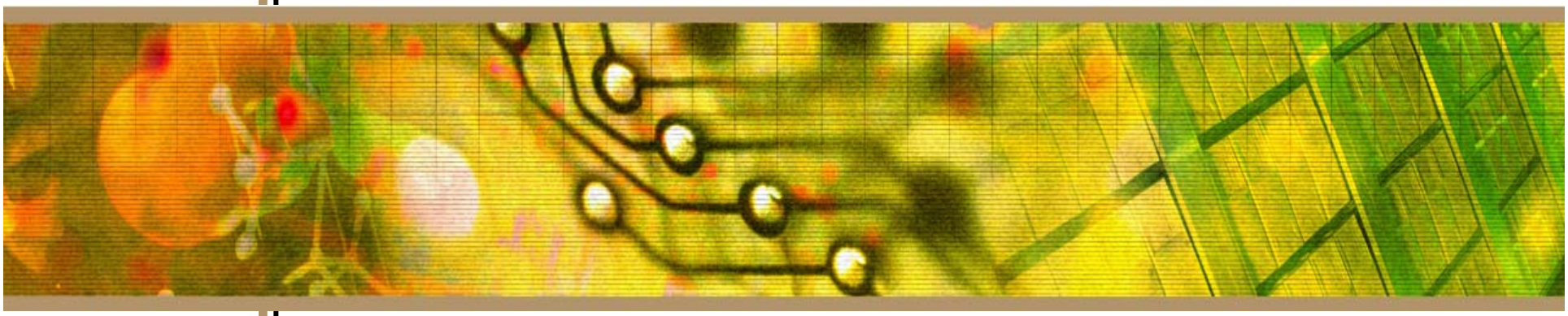
PURDUE
UNIVERSITY

Basics of Router Administration



Presented by Brad DeVine
Senior Network Engineer

SECURE PURDUE

PURDUE UNIVERSITY

Introduction

- Reason for Presentation
  - Best Practices for Securing Network Devices
  - Important data is not stored on our network devices. But an intruder or attacker can shut down business by hijacking or interfering with them.
  - They can change access controls.
  - They can gain access to otherwise secured networks and resources.
  - Can Redirect/Mirror traffic to another location.
- Outline of Topics
  - The different types of network devices, and how they're administered.
  - What bad things can happen when a network device is compromised?
  - What measures can an admin take to prevent problems?

PURDUE UNIVERSITY

Different Network Devices and How They're Administered

- Routers
  - Separate and connect different IP subnets
  - Each subnet is a broadcast domain
  - Routers make their forwarding decisions based on the destination IP address
  - They build the forwarding tables by exchanging info with other routers or the administrator

PURDUE UNIVERSITY

Different Network Devices and How They're Administered

- Hubs
  - Provide more network ports for users
  - Bandwidth is shared among all users, including the router
  - Have no intelligence - they don't make forwarding decisions. Just read and repeat.
  - As a result, every host attached to the hub sees everyone else's traffic. A hacker's dream.

PURDUE UNIVERSITY

Different Network Devices and How They're Administered

- Switches (Bridges)
  - Provide more ports like hubs. But each port has its own dedicated bandwidth.
  - And each port only sees traffic destined for it.
  - Broadcasts and unknown frames are the exception.
  - If you want to Sniff a switch ports, it must be configured by an admin.
  - They make their forwarding decisions based on destination mac-address.
  - They build their forwarding tables by reading the source mac-addresses.

PURDUE UNIVERSITY

Different Network Devices and How They're Administered

- Firewalls
  - Basically routers with much better traffic inspection capabilities.
  - Can be layer 3, just like a router.
  - Or they can be layer 2, where the inside and outside interfaces are on the same subnet.
  - Can be stand alone appliances, a blade within another switch chassis, or software within another device.

PURDUE UNIVERSITY

Different Network Devices and How They're Administered

- Wireless Access Points
  - Just a network switch, where one side is Ethernet, and the other is wireless.
  - Wireless routers also exist.
  - There are a host of wireless related vulnerabilities. I won't be talking about them today, because that's not my expertise.
  - But know that if an intruder gains access to an access point, it can be a jumping off point to other network devices.

PURDUE UNIVERSITY

Different Network Devices and How They're Administered

- Evolution of Network Devices
  - A common setup was a router with a hub, or Coax thicknet cable attached.
  - Everyone on hub was on the same subnet.
  - Then came vlan aware switches. Hosts could choose which subnet/vlan to be a member of.
  - Now LAN routers don't usually have physical ports. The gateway, or "dot 1" address is usually a virtual port within a blade in the chassis.
  - In fact, routing, fire walling, VPN, and wireless services are often contained as software functions within a large switch chassis.

PURDUE UNIVERSITY

Different Network Devices and How They're Administered

- How Network Devices are Administered
  - The administration is usually common.
  - On physical boxes, there's a console port to attach a dumb terminal or terminal program.
  - Blades in a chassis don't have the physical port. But you can access them virtually from within the parent chassis.
  - Once initially set up, you can TELNET/SSH/SNMP/HTTPS from across the network.

- Physical Security
  - Console port rarely has authentication on it.
  - It must be behind a physical barrier.
  - If a network device can't be reached over the network, you must use the console to fix it.
  - That creates a chicken before the egg scenario if authentication to a network server is set up.
  - The solution is to use local usernames, or no password at all.
  - It's a risk. But if you have physical access to the console, you can get in to the device, no matter what.

What Bad Things Can Happen? How Do We Prevent Them?

Part I

- Physical Security Cont.
  - All ITaP switches are behind keyed or card swiped doors.
  - But an intruder can still find a way in. So what do we do?
  - The solution is to use different privilege levels on the devices.
  - The console gives read-only access. And even that is limited.
  - If you want to do some damage, you must have privileged level access. Only a select few engineers have it.

What Bad Things Can Happen? How Do We Prevent Them?

Part I

- AUX Ports
  - These are just like console ports, but pinned out for a modem to be attached.
  - Authentication is necessary, due to the risk of war dialing programs.
  - We don't generally use the AUX port. We have other ways of doing this.
- Virtual Terminals
  - VTY's let you telnet or SSH into a device and get a command shell.
  - Cisco devices provide 15 at a time by default. You don't really want more than one person changing things at once though.
  - Can be secured via username/password, or PKI using Smart Cards.
  - The main security problem with them is that telnet is enabled by default. Telnet is not secure.

What Bad Things Can Happen? How Do We Prevent Them?

Part I

- Physical and Logical Separation of Network Devices
  - Some organizations have separate networks for sensitive data.
  - The components can be physically separate, like in the DOD.
  - Or they can be logically separate, like we use in the Data Centers.
  - The network devices set aside separate memory, CPU, etc. for the sensitive network. The normal network has no knowledge of the others.
- Specific Administration Attacks
  - "Write erase / reload" One of our worst nightmares. It would take an army of students to correct.
  - Setting up a SPAN, or Sniffer, port to redirect traffic to a rogue workstation.
  - Setting up RSPAN to a workstation across the network. This can also have a DOS effect by doubling the bandwidth across the links.

What Bad Things Can Happen? How Do We Prevent Them?

Part II

- Denial of Service Attacks
  - A simple one is to use up all the virtual terminals to prevent legit admins from getting in.
  - But you don't need to take over administration of a network device to cause problems.
- Device Control Plane vs. User Plane
  - User plane is set of resources on a device that normal user traffic goes across.
  - Most of this traffic is not seen by the device CPU.
  - In higher end switches, this is done in hardware.
  - On lower end devices, separate memory, CPU, etc. is set aside.

What Bad Things Can Happen? How Do We Prevent Them?

Part II

- Device Control Plane vs. User Plane (cont.)
  - Control plane is set of resources used for traffic that must be seen by the device itself
  - This includes:
    - » Management Traffic
    - » Broadcasts like ARP
    - » Spanning-tree Frames
    - » Packets with IP options set
    - » Unknown destination traffic
  - If attackers can saturate the control plane, the entire device can be rendered useless.
  - Routing and Switching tables would be become out of date and useless. And legit administrators couldn't get in to fix it.
  - The best way to prevent this is to use different subnets for user and management traffic.

What Bad Things Can Happen? How Do We Prevent Them?

Part II

- Using Quality of Service to Mitigate DOS Attacks.
  - QoS marks important traffic and gives it priority.
  - What is "priority"? That's up to the organization. But routing updates, management traffic, and the like are essential.
  - QoS "priority" only kicks in when the network is saturated, like during a DOS attack.
  - During that time, user traffic is selectively dropped in favor of the "important" traffic.
  - This process is called Control Plane Policing
- QoS Scavenger Class
  - Marks any traffic above, say 10% utilization, with lower priority.
  - Has zero effect during normal operation.
  - During times of trouble, the traffic above 10% is dropped.
  - The theory is that most user ports never sustain above 5% utilization. That is, until they become infected.
  - This would never be used on server ports.

What Bad Things Can Happen? How Do We Prevent Them?

Part II

- The Spanning-Tree Protocol
  - If a switch becomes so saturated, it stops processing spanning-tree, the entire network can come crashing down.
  - In a network, redundancy is good.
    - » Routers handle redundant links with ease.
    - » Switches need extra help.
    - » If you start adding extra links in between switches, frames can loop endlessly between them.
    - » This is why chaining hubs / Linksys Routers together is bad. They don't speak spanning-tree.
    - » Spanning-tree negotiates between the switches to choose which links to use, and which to keep in standby.

What Bad Things Can Happen? How Do We Prevent Them? continued

Part II

- In a routed network, the layer 3 header has TTL field that keeps packets from looping around endlessly.
- The layer 2 frame has no such mechanism.
- It's also possible for a host to claim to be the root of the spanning-tree. Then all traffic flows through them.
- There are commands to prevent all these things.

What Bad Things Can Happen? How Do We Prevent Them?

Part II

- Other Common Attacks and Problems
  - CAM Table Overflows
  - VLAN Hopping
  - ARP Spoofing
  - VTP Death
  - DHCP Starvation.

PURDUE UNIVERSITY

General Precautions

- General Device Hardening
  - Disable unnecessary UNIX Services.
  - Disable unneeded info towards the rest of the network like CDP/FDP info.
  - Disable unneeded IP Services on routers like proxy-arp and directed-broadcasts.
  - Use source-address validation to prevent IP spoofing.
  - Use access-lists on VTY's and for SNMP. Read-only is a must.
  - Use a AAA server for authorizing command and recording accounting info.
  - Use MD5 hashed passwords to prevent shoulder surfing.
  - Use MD5 authentication between routers to prevent routing table corruption.
  - Disable unneeded ICMP messages that give attackers more info than they need to know.

PURDUE
UNIVERSITY

Questions?